G.N. 1226

INSURANCE ORDINANCE (CHAPTER 41) AND ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING ORDINANCE (Chapter 615)

Pursuant to section 133(1) of the Insurance Ordinance (Chapter 41) and section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Chapter 615), the revised Guideline on Anti-Money Laundering and Counter-Terrorist Financing ('GL3') is published by the Insurance Authority.

The revised Guideline will come into operation on 1 March 2018, and shall supersede the previous version of the Guideline.

23 February 2018 John LEUNG *Chief Executive Officer Insurance Authority*

GL3

Guideline on Anti-Money Laundering and Counter-Terrorist Financing

(For authorized insurers, reinsurers, appointed insurance agents and authorized insurance brokers carrying on or advising on long term business)

Insurance Authority

March 2018

Contents Page

Chapter 1 – OVERVIEW		
Introduction		
	1.1	The Guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap. 615 (the AMLO) and section 133 of the Insurance Ordinance, Cap. 41 (the IO), and shall take effect from 1 March 2018.
	1.2	Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of this Guideline. Interpretation of other words or phrases should follow those set out in the AMLO and the IO.
	1.3	This Guideline is issued by the Insurance Authority for giving guidance to authorized insurers, reinsurers, appointed insurance agents and authorized insurance brokers carrying on or advising on long term business (hereinafter referred to as "insurance institutions ("IIs")"). In general, the guidance provided in the Guideline in Chapters 1-10 to IIs is not different from the guidance provided by other relevant authorities (RAs) under their respective regulatory regimes. To the extent that the Insurance Authority sees fit to provide supplementary guidance in Chapters 1-10, such will be put in italics for ease of identification.
	1.4	The Guideline is intended for use by financial institutions (FIs) and their officers and staff. The purposes of the Guideline are to: (a) provide a general background on the subjects of money laundering and terrorist financing (ML/TF), including a summary of the main provisions of the applicable anti-money laundering and counter-financing of terrorism (AML/CFT) legislation in Hong Kong; and (b) provide practical guidance to assist FIs and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements.
	1.5	The relevance and usefulness of the Guideline will be kept under review and it may be necessary to issue amendments from time to time.
	1.6	Given the significant differences that exist in the organisational and legal structures of different FIs as well as the nature and scope of the business activities conducted by them, there exists no single set of universally applicable implementation measures. It must also be

		emphasized that the contents of the Guideline is neither intended to, nor should be construed as, an exhaustive list of the means of meeting the statutory and regulatory requirements.
	1.7	This Guideline provides guidance in relation to the operation of the provisions of Schedule 2 to the AMLO (Schedule 2). This will assist FIs to meet their legal and regulatory obligations when tailored by FIs to their particular business risk profile. Departures from this Guidance, and the rationale for so doing, should be documented, and FIs will have to stand prepared to justify departures to the RAs.
s.7, AMLO	1.8	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.
	1.8a	*In addition, a failure to comply with any provision of this Guideline by IIs may reflect adversely on the fitness and properness of their directors and controllers[1], and may result in disciplinary action taken against IIs.*
The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.9	The term "money laundering" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means an act intended to have the effect of making any property: (a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or (b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.
	1.10	There are three common stages in the laundering of money, and they frequently involve numerous transactions. An FI should be alert to any such sign for potential criminal activities. These stages are:

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

		(a) Placement - the physical disposal of cash proceeds derived from illegal activities; (b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and (c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.
s.1, Sch. 1, AMLO	1.11	The term "terrorist financing" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means: (a) the provision or collection, by any means, directly or indirectly, of any property – (i) with the intention that the property be used; or (ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or (c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.
	1.12	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		
	1.12a	*The insurance industry is vulnerable to ML and TF. The inherent characteristics of insurance products may give rise to ML risks unique to the insurance industry. 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 possibly against payment before maturity or surrender, in order that payments can be made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may only be one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.
	1.12b	*Examples of the type of long term insurance contracts that are vulnerable as a vehicle for laundering money or financing terrorism are products such as:* *(a) unit-linked or with profit single premium contracts;* *(b) single premium life insurance policies that store cash value;* *(c) fixed and variable annuities; and* *(d) (second hand) endowment policies.*
	1.12c	*ML and TF using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives or by the misuse of normal reinsurance transactions. Examples include:* • *the deliberate placement via the insurer of the proceeds of crime or terrorist property with reinsurers in order to disguise the source of funds;* • *the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding;* • *the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist property with legitimate reinsurers.*
	1.12d	*Insurance intermediaries[2] 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*

[2] *Insurance intermediaries refer to appointed insurance agents or authorized insurance brokers carrying on or advising on long term insurance business in Hong Kong.*

		ML or TF. The intermediaries themselves could have been set up to channel illegitimate funds to insurers.
Legislation concerned with money laundering and terrorist financing		
	1.13	The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989 that sets the international AML standards. Its mandate was expanded in October 2001 to combat the financing of terrorism. 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 uncooperative jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Many major economies have joined the FATF which has developed into a global network for international cooperation that facilitates exchanges between member jurisdictions. As a member of the FATF, Hong Kong is obliged to implement the AML requirements as promulgated by the FATF, which include the 40 Recommendations and the Nine Special Recommendations (hereafter referred to collectively as "FATF's Recommendations")[3] and it is important that Hong Kong complies with the international AML standards in order to maintain its status as an international financial centre.
	1.14	The four main pieces of legislation in Hong Kong that are concerned with ML/TF are the AMLO, the Drug Trafficking (Recovery of Proceeds) Ordinance (the DTROP), the Organized and Serious Crimes Ordinance (the OSCO) and the United Nations (Anti-Terrorism Measures) Ordinance (the UNATMO). It is very important that FIs and their officers and staff fully understand their respective responsibilities under the different legislation.
<u>AMLO</u>		
s.23, Sch. 2	1.15	The AMLO imposes requirements relating to customer due diligence (CDD) and record-keeping on FIs and provides RAs with the powers to supervise compliance with these requirements and other requirements under the AMLO. In addition, section 23 of Schedule 2 requires FIs to take all reasonable measures (a) to ensure that proper safeguards exist to prevent a contravention of any requirement under Parts 2 and 3 of Schedule 2; and (b) to mitigate ML/TF risks.

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

s.5, AMLO	1.16	The AMLO makes it a criminal offence if an FI (1) knowingly; or (2) with the intent to defraud any RA, contravenes a specified provision of the AMLO. The "specified provisions" are listed in section 5(11) of the AMLO. If the FI knowingly contravenes a specified provision, it is liable to a maximum term of imprisonment of 2 years and a fine of $1 million. If the FI contravenes a specified provision with the intent to defraud any RA, it is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.5, AMLO	1.17	The AMLO also makes it a criminal offence if a person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI (1) knowingly; or (2) with the intent to defraud the FI or any RA, causes or permits the FI to contravene a specified provision in the AMLO. If the person who is an employee of an FI or is employed to work for an FI or is concerned in the management of an FI knowingly contravenes a specified provision he is liable to a maximum term of imprisonment of 2 years and a fine of $1 million upon conviction. If that person does so with the intent to defraud the FI or any RA he is liable to a maximum term of imprisonment of 7 years and a fine of $1 million upon conviction.
s.21, AMLO	1.18	RAs may take disciplinary actions against FIs for any contravention of a specified provision in the AMLO. The disciplinary actions that can be taken include publicly reprimanding the FI; ordering the FI to take any action for the purpose of remedying the contravention; and ordering the FI to pay a pecuniary penalty not exceeding the greater of $10 million or 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention.
DTROP		
	1.19	The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.
OSCO		
	1.20	The OSCO, among other things: (a) gives officers of the Hong Kong Police 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 money laundering 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		
	1.21	The UNATMO is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001 of the United Nations Security Council (UNSC) aimed at preventing the financing of terrorist acts. Besides the mandatory elements of the UNSC Resolution 1373, the UNATMO also implements the more pressing elements of the FATF's special recommendations on terrorist financing.
s.25, DTROP & OSCO	1.22	Under the DTROP and the OSCO, a person commits an offence if he deals with any property knowing or having reasonable grounds to believe it to represent any person's proceeds of drug trafficking or of an indictable offence respectively. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine of $5 million.
s.6, 7, 8, 13 & 14, UNATMO	1.23	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	1.24	The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of $50,000 upon conviction.
s.25A, DTROP & OSCO, s.12	1.25	"Tipping off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter

& 14, UNATMO		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.

Chapter 2 – AML/CFT SYSTEMS AND BUSINESS CONDUCTED OUTSIDE HONG KONG		
AML/CFT systems		
s.23(a) & (b), Sch. 2	2.1	FIs must take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2. To ensure compliance with this requirement, FIs should implement appropriate internal AML/CFT policies, procedures and controls (hereafter collectively referred to as "AML/CFT systems").
Risk factors		
	2.2	While no system will detect and prevent all ML/TF activities, FIs should establish and implement adequate and appropriate AML/CFT systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved.
Product/service risk		
	2.3	An FI should consider the characteristics of the products and services that it offers and the extent to which these are vulnerable to ML/TF abuse. In this connection, an FI should assess the risks of any new products and services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes) before they are introduced and ensure appropriate additional measures and controls are implemented to mitigate and manage the associated ML/TF risks.
Delivery/distribution channel risk		
	2.4	An FI should also consider its delivery/distribution channels and the extent to which these are vulnerable to ML/TF abuse. These may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the business relationship between the customer and an FI may become indirect.
Customer risk		
	2.5	When assessing the customer risk, FIs should consider who their customers are, what they do and any other information that may suggest the customer is of higher risk.

	2.6	An FI should be vigilant where the customer is of such a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it or the business/industrial sector to which a customer has business connections is more vulnerable to corruption. Examples include: (a) companies that can be incorporated without the identity of the ultimate underlying principals being disclosed; (b) certain forms of trusts or foundations where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed; (c) the provision for nominee shareholders; and (d) companies issuing bearer shares.
	2.7	An FI should also consider risks inherent in the nature of the activity of the customer and the possibility that the transaction may itself be a criminal transaction. For example, the arms trade and the financing of the arms trade is a type of activity that poses multiple ML and other risks, such as: (a) corruption risks arising from procurement contracts; (b) risks in relation to politically exposed persons (PEPs); and (c) terrorism and TF risks as shipments may be diverted.
Country risk		
	2.8	An FI should pay particular attention to countries or geographical locations of operation with which its customers and intermediaries are connected where they are subject to high levels of organized crime, increased vulnerabilities to corruption and inadequate systems to prevent and detect ML/TF. When assessing which countries are more vulnerable to corruption, FIs may make reference to publicly available information or relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations (an example of which is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption).
<u>Effective controls</u>		
	2.9	To ensure proper implementation of such policies and procedures, FIs should have effective controls covering: (a) senior management oversight; (b) appointment of a Compliance Officer (CO) and a Money

		Laundering Reporting Officer (MLRO)[4]; (c) compliance and audit function; and (d) staff screening and training[5].
Senior management oversight		
	2.10	The senior management of any FI is responsible for managing its business effectively; in relation to AML/CFT this includes oversight of the functions described below.
	2.11	Senior management should: (a) be satisfied that the FI's AML/CFT systems are capable of addressing the ML/TF risks identified; (b) appoint a director or senior manager as a CO who has overall responsibility for the establishment and maintenance of the FI's AML/CFT systems; and (c) appoint a senior member of the FI's staff as the MLRO who is the central reference point for suspicious transaction reporting.
	2.12	In order that the CO and MLRO can discharge their responsibilities effectively, senior management should, as far as practicable, ensure that the CO and MLRO are: (a) subject to constraint of size of the FI, independent of all operational and business functions; (b) normally based in Hong Kong; (c) of a sufficient level of seniority and authority within the FI; (d) provided with regular contact with, and when required, direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risks of ML/TF; (e) fully conversant in the FI's statutory and regulatory requirements and the ML/TF risks arising from the FI's business; (f) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from RAs); and (g) 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

[4] The role and functions of an MLRO are detailed at paragraphs 7.19-7.30. For some FIs, the functions of the CO and the MLRO may be performed by the same staff member.

[5] For further guidance on staff training see Chapter 9.

		same status).
Compliance officer and money laundering reporting officer		
	2.13	The principal function of the CO is to act as the focal point within an FI for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed. In particular, the CO should assume responsibility for: (a) developing and/or continuously reviewing the FI's AML/CFT systems to ensure they remain up-to-date and meet current statutory and regulatory requirements; and (b) the oversight of all aspects of the FI's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary.
	2.14	In order to effectively discharge these responsibilities, a number of areas should be considered. These include: (a) the means by which the AML/CFT systems are managed and tested; (b) the identification and rectification of deficiencies in the AML/CFT systems; (c) reporting numbers within the systems, both internally and disclosures to the Joint Financial Intelligence Unit (JFIU); (d) the mitigation of ML/TF risks arising from business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations; (e) the communication of key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; (f) changes made or proposed in respect of new legislation, regulatory requirements or guidance; (g) compliance with any requirement under Part 2 or 3 of Schedule 2 in overseas branches and subsidiary undertakings and any guidance issued by RAs in this respect; and (h) AML/CFT staff training.
	2.15	The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions performed are expected to include: (a) reviewing all 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) maintaining all records related to such internal reviews; (c) providing guidance on how to avoid "tipping off" if any disclosure is made; and (d) acting as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.
Compliance and audit function		
	2.16	Where practicable, an FI should establish an independent compliance and audit function which should have a direct line of communication to the senior management of the FI.
	2.17	The compliance and audit function of the FI should regularly review the AML/CFT systems, e.g. sample testing, (in particular, the system for recognizing and reporting suspicious transactions) to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the FI's business. Where appropriate, the FI should seek a review from external sources.
Staff screening		
	2.18	FIs must establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees.
Business conducted outside Hong Kong		
s.22(1), Sch. 2	2.19	A Hong Kong-incorporated FI with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure that all branches and subsidiary undertakings that carry on the same business as an FI in a place outside Hong Kong have procedures in place to comply with the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2 to the extent permitted by the law of that place. The FI should communicate the group policy to its overseas branches and subsidiary undertakings.
s.22(2), Sch. 2	2.20	When a branch or subsidiary undertaking of an FI outside Hong Kong is unable to comply with requirements that are similar to those imposed under Parts 2 and 3 of Schedule 2 because this is not permitted by local laws, the FI must: (a) inform the RA 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 above requirements.

s.25A, OSCO & DTROP	2.21	Suspicion that property in whole, or partly directly or indirectly represents the proceeds of an indictable offence, should normally be reported within the jurisdiction where the suspicion arises and where the records of the related transactions are held. However, in certain cases, e.g. when the account is domiciled in Hong Kong, reporting to the JFIU[6] may be required in such circumstances, but only if section 25A of OSCO/DTROP applies.

[6] Section 25(4) of the OSCO stipulates that an indictable offence includes conduct outside Hong Kong which would constitute an indictable offence if it had occurred in Hong Kong. Therefore, where an FI in Hong Kong has information regarding money laundering, irrespective of the location, it should consider seeking clarification with and making a report to the JFIU.

Chapter 3 – RISK-BASED APPROACH		
Introduction		
	3.1	The risk-based approach to CDD and ongoing monitoring (RBA) is recognized as an effective way to combat ML/TF. The general principle of an RBA is that where customers are assessed to be of higher ML/TF risks, FIs should take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower, simplified measures may be applied. The use of an RBA has the advantage of allowing resources to be allocated in the most efficient way directed in accordance with priorities so that the greatest risks receive the highest attention.
General requirement		
	3.2	FIs should determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified. The measures must however comply with the legal requirements of the AMLO. The RBA will enable FIs to subject customers to proportionate controls and oversight by determining: (a) the extent of the due diligence to be performed on the direct customer; the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer; (b) the level of ongoing monitoring to be applied to the relationship; and (c) measures to mitigate any risks identified. For example, the RBA may require extensive CDD for high risk customers, such as an individual (or corporate entity) whose source of wealth and funds is unclear or who requires the setting up of complex structures. FIs should be able to demonstrate to the RAs that the extent of CDD and ongoing monitoring is appropriate in view of the customer's ML/TF risks.

	3.3	There are no universally accepted methodologies that prescribe the nature and extent of an RBA. However, an effective RBA does involve identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An effective RBA will allow FIs to exercise reasonable business judgment with respect to their customers. An RBA should not be designed to prohibit FIs from engaging in transactions with customers or establishing business relationships with potential customers, but rather it should assist FIs to effectively manage potential ML/TF risks.
Customer acceptance/risk assessment		
	3.4	FIs may assess the ML/TF risks of individual customers by assigning a ML/TF risk rating to their customers.
	3.5	While there is no agreed upon set of risk factors and no one single methodology to apply these risk factors in determining the ML/TF risk rating of customers, relevant factors to be considered may include the following: <u>1. Country risk</u> Customers with residence in or connection with high-risk jurisdictions[7] for example: (a) those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; (b) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations; (c) countries which are vulnerable to corruption; and (d) those countries that are believed to have strong links to terrorist activities. In assessing country risk associated with a customer, consideration may be given to local legislation (United Nations Sanctions Ordinance (UNSO), UNATMO), data available from the United Nations, the International Monetary Fund, the World Bank, the FATF, etc. and the FI's own experience or the experience of other group entities (where the FI is part of a multi-national group) which may have indicated weaknesses in other jurisdictions.

[7] Guidance on jurisdictions that do not or insufficiently apply the FATF's Recommendations or otherwise pose a higher risk is provided at paragraphs 4.15.

		2. Customer risk The following are examples of customers who might be considered to carry lower ML/TF risks: (a) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and (b) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control. However, some customers, by their nature or behaviour might present a higher risk of ML/TF. Factors might include: (a) the public profile of the customer indicating involvement with, or connection to, PEPs; (b) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale; (c) a request to use numbered accounts or undue levels of secrecy with a transaction; (d) involvement in cash-intensive businesses; (e) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities; and (f) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified. 3. Product/service risk Factors presenting higher risk might include: (a) services that inherently have provided more anonymity; and (b) ability to pool underlying customers/funds. 4. Delivery/distribution channel risk The distribution channel for products may alter the risk profile of a customer. This may include sales through online, postal or telephone channels where a non-face-to-face account opening approach is used. Business sold through intermediaries may also increase risk as the

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

Chapter 4 – CUSTOMER DUE DILIGENCE		
4.1 Introduction to CDD		
	4.1.1	The AMLO defines what CDD measures are (see paragraph 4.1.3) and also prescribes the circumstances in which an FI must carry out CDD (see paragraph 4.1.9). As indicated in the AMLO, FIs may also need to conduct additional measures (referred to as enhanced customer due diligence (EDD) hereafter) or could conduct simplified customer due diligence (SDD) depending on specific circumstances. This chapter sets out the expectations of RAs in this regard and suggests ways that these expectations may be met. Wherever possible, the guideline gives FIs a degree of discretion in how they comply with the AMLO and put in place procedures for this purpose.
	4.1.2	CDD information is a vital tool for recognising whether there are grounds for knowledge or suspicion of ML/TF.
s.2, Sch. 2	4.1.3	The following are CDD measures applicable to an FI: (a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information (see paragraphs 4.2); (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust[8], measures to enable the FI to understand the ownership and control structure of the legal person or trust (see paragraphs 4.3); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the FI unless the purpose and intended nature are obvious (see paragraphs 4.6); and (d) if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information; and (ii) verify the person's authority to act on behalf of the customer (see paragraphs 4.4).
	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.

[8] 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.

	4.1.4a	*For the insurance industry, the term "customer" refers to policy holder.*
	4.1.5	In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, the FI should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship. Due consideration should also be given to the measures set out in Chapter 3.
	4.1.6	FIs should adopt a balanced and common sense approach with regard to customers connected with jurisdictions which do not or insufficiently apply the FATF recommendations (see paragraphs 4.15). While extra care may well be justified in such cases, unless a RA has, through a "notice in writing", imposed a general or specific requirement (see paragraph 4.16.1), it is not a requirement that FIs should refuse to do any business with such customers or automatically classify them as high risk and subject them to EDD process. Rather, FIs should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.
s.1, Sch. 2	4.1.7	"Business relationship" between a person and an FI is defined in the AMLO as a business, professional or commercial relationship: (a) that has an element of duration; or (b) that the FI, at the time the person first contacts it in the person's capacity as a potential customer of the FI, expects to have an element of duration.
s.1, Sch. 2	4.1.8	The term "occasional transaction" is defined in the AMLO as a transaction between an FI and a customer who does not have a business relationship with the FI.[9]
s.3(1), Sch. 2	4.1.9	CDD requirements should apply: (a) at the outset of a business relationship; (b) before performing any occasional transaction[10]: (i) equal to or exceeding an aggregate value of $120,000, whether carried out in a single operation or several operations that

[9] It should be noted that "occasional transactions" do not apply to the insurance and securities sectors.

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

		appear to the FI to be linked; or (ii) a wire transfer equal to or exceeding an aggregate value of $8,000, whether carried out in a single operation or several operations that appear to the FI to be linked; (c) when the FI suspects that the customer or the customer's account is involved in ML/TF[11]; 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.
	4.1.10	FIs should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of $8,000 for wire transfers and $120,000 for other types of transactions. Where FIs become aware that these thresholds are met or exceeded, full CDD procedures must be applied.
	4.1.11	The factors linking occasional transactions are inherent in the characteristics of the transactions – for example, where several payments are made to the same recipient from one or more sources over a short period, where a customer regularly transfers funds to one or more destinations. In determining whether the transactions are in fact linked, FIs should consider these factors against the timeframe within which the transactions are conducted.
4.2 Identification and verification of the customer's identity		
s.2(1)(a), Sch. 2	4.2.1	The FI must identify the customer and verify the customer's identity by reference to documents, data or information provided by a reliable and independent source[12]: (a) a governmental body; (b) the RA or any other RA; (c) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or (d) any other reliable and independent source that is recognized by the RA.
4.3 Identification and verification of a beneficial owner		
s.1 & s.2(1)(b), Sch. 2	4.3.1	A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. An FI must identify any beneficial owner in relation

[11] This criterion applies irrespective of the $120,000 threshold.

[12] See Appendix A which contains a list of documents recognised by the RAs as independent and reliable sources for identity verification purposes.

		to a customer, and, based on its assessment of the ML/TF risks, take reasonable measures to verify the beneficial owner's identity so that the FI is satisfied that it knows who the beneficial owner is. However, the verification requirements under the AMLO are different for a customer and a beneficial owner.
	4.3.2	Where an individual is identified as a beneficial owner, the FI should endeavour to obtain the same identification information as at paragraph 4.8.1.
	4.3.3	In respect of a customer who is an individual, there is no requirement on FIs to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.
	4.3.4	For beneficial owners, FIs should obtain the residential address (and permanent address if different) and may adopt a risk-based approach to determine the need to take reasonable measures to verify the address, taking account of the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.
4.4 Identification and verification of a person purporting to act on behalf of the customer		
s.2(1)(d), Sch. 2	4.4.1	If a person purports to act on behalf of the customer, FIs must: (i) identify the person and take reasonable measures to verify the person's identity on the basis of documents, data or information provided by- (A) a governmental body; (B) the relevant authority or any other relevant authority; (C) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority; or (D) any other reliable and independent source that is recognised by the relevant authority; and (ii) verify the person's authority to act on behalf of the customer.
	4.4.2	The general requirement is to obtain the same identification information as set out in paragraph 4.8.1. In taking reasonable measures to verify the identity of persons purporting to act on behalf of customers (e.g. authorized account signatories and attorneys), the FI should refer to the documents and other means listed in Appendix A wherever possible. As a general rule FIs should identify and verify the

		identity of those authorized to give instructions for the movement of funds or assets.
s.2(1)(d)(ii), Sch. 2	4.4.3	FIs should obtain written authority[13] to verify that the individual purporting to represent the customer is authorized to do so.
s.2(1)(d), Sch. 2	4.4.4	FIs may on occasion encounter difficulties in identifying and verifying signatories of customers that may have long lists of account signatories, particularly if such customers are based outside Hong Kong. In such cases, FIs may adopt a risk-based approach in determining the appropriate measures to comply with these requirements; for example in respect of verification of account signatories related to a customer, such as an FI or a listed company[14], FIs could adopt a more streamlined approach. The provision of a signatory list[15], recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified (e.g. compliance, audit or human resources), may be sufficient to demonstrate compliance with these requirements. Another option, mainly relevant to overseas customers and which may be considered in conjunction with or separately from reducing the signatories list, is the use of intermediaries in accordance with section 18 of Schedule 2.
4.4a Special requirements for insurance policies		
s.11(1), Sch. 2	*4.4a.1*	*An II must, 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*

[13] For corporation, FIs should obtain the board resolution or similar written authority.
[14] Having regard to the advice provided at paragraphs 4.15.
[15] Or equivalent.

		the terms of the insurance policy, *whichever is the earlier.*
s.11(2), Sch. 2	*4.4a.2*	*An II must carry out the measures specified in paragraphs 4.4a.3 and 4.4a.4:* *(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	*4.4a.3*	*An II must 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 RA or any other RA;* *(c) an authority in a place outside Hong Kong that performs functions similar to those of the RA or any other RA; or* *(d) any other reliable and independent source that is recognized by the RA.*
s.11(3)(b), Sch. 2	*4.4a.4*	*Where the beneficiary is a legal person or trust, an II must:* *(i) identify its beneficial owners; and* *(ii) 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.*
	4.4a.5	*Where an II is unable to comply with paragraphs 4.4a.1 to 4.4a.4 above, it should consider making a suspicious transaction report.*
	4.4a.6	*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 monies should also be the subjects of identification and verification.*
4.4b Requirements for reinsurance		
	4.4b.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.*

4.5 Characteristics and evidence of identity		
	4.5.1	No form of identification can be fully guaranteed as genuine or representing correct identity and FIs should recognise that some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, FIs should take whatever practical and proportionate steps are available to establish whether the document offered is genuine, or has been reported as lost or stolen. This may include searching publicly available information, approaching relevant authorities (such as the Immigration Department through its hotline) or requesting corroboratory evidence from the customer. Where suspicion cannot be eliminated, the document should not be accepted and consideration should be given to making a report to the authorities. Where documents are in a foreign language, appropriate steps should be taken by the FI to be reasonably satisfied that the documents in fact provide evidence of the customer's identity (e.g. ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person).
4.6 Purpose and intended nature of business relationship		
s.2(1)(c), Sch. 2	4.6.1	An FI must understand the purpose and intended nature of the business relationship. In some instances, this will be self-evident, but in many cases, the FI may have to obtain information in this regard.
	4.6.2	Unless the purpose and intended nature are obvious, FIs should obtain satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the account opening documentation. Depending on the FI's risk assessment of the situation, information that might be relevant may include: (a) nature and details of the business/occupation/employment; (b) the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be); (c) location of customer; (d) the expected source and origin of the funds to be used in the relationship; and (e) initial and ongoing source(s) of wealth or income.

	4.6.3	This requirement also applies in the context of non-residents. While the vast majority of non-residents seek business relationships with FIs in Hong Kong for perfectly legitimate reasons, some non-residents may represent a higher risk for ML/TF. An FI should understand the rationale for a non-resident to seek to establish a business relationship in Hong Kong.
4.7 Timing of identification and verification of identity		
General requirement		
s.3(1), Sch. 2	4.7.1	An FI must complete the CDD process before establishing any business relationship or before carrying out a specified occasional transaction (exceptions are set out at paragraph 4.7.4).
s.3(4), Sch. 2	4.7.2	Where the FI is unable to complete the CDD process in accordance with paragraph 4.7.1, it must not establish a business relationship or carry out any occasional transaction with that customer and should assess whether this failure provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.
Delayed identity verification during the establishment of a business relationship		
	4.7.3	Customer identification information (and information on any beneficial owners) and information about the purpose and intended nature of the business relationship should be obtained before the business relationship is entered into.
s.3(2), (3) & (4)(b), Sch. 2	4.7.4	However, FIs may, exceptionally, verify the identity of the customer and any beneficial owner after establishing the business relationship, provided that: (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed; (b) it is necessary not to interrupt the normal course of business with the customer; (c) verification is completed as soon as reasonably practicable; and (d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.
	4.7.5	Examples of situations where it may be necessary not to interrupt the normal conduct of business include: (a) securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very

		rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed; and (b) life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policy holder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.
	4.7.5a	*Having considered the difficulty for IIs to obtain copies of the identification documents of individual customers when the sales process occurs outside the office, IIs 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 as stated in paragraph 4.7.8 or at or before the time of payout, whichever is the earlier.*
	4.7.6	Where a customer is permitted to utilise the business relationship prior to verification, FIs should adopt appropriate risk management policies and procedures concerning the conditions under which this may occur. These policies and procedures should include: (a) establishing timeframes for the completion of the identity verification measures; (b) regular monitoring of such relationships pending completion of the identity verification, and keeping senior management periodically informed of any pending completion cases; (c) obtaining all other necessary CDD information; (d) ensuring verification of identity is carried out as soon as it is reasonably practicable; (e) advising the customer of the FI's obligation to terminate the relationship at any time on the basis of non-completion of the verification measures; (f) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification; and (g) ensuring that funds are not paid out to any third party. Exceptions[16] may be made to allow payments to third parties subject to the following conditions:

[16] It should be noted that the exceptions do not apply to insurance sector.

		(i) there is no suspicion of ML/TF; (ii) the risk of ML/TF is assessed to be low; (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and (iv) the names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.
	4.7.7	The FI must not use this concession for the circumvention of CDD procedures, in particular, where it: (a) has knowledge or a suspicion of ML/TF; (b) becomes aware of anything which causes it to doubt the identity or intentions of the customer or beneficial owner; or (c) the business relationship is assessed to pose a higher risk.
Failure to complete verification of identity		
s.3(4)(b), Sch. 2	4.7.8	Verification of identity should be concluded within a reasonable timeframe[17]. Where verification cannot be completed within such a period, the FI should as soon as reasonably practicable suspend or terminate the business relationship unless there is a reasonable explanation for the delay. Examples of reasonable timeframe are: (a) the FI completing such verification no later than 30 working days after the establishment of business relations; (b) the FI suspending business relations 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 relations; and (c) the FI terminating business relations with the customer if such verification remains uncompleted 120 working days after the establishment of business relations.
s.25A, DTROP & OSCO, s.12, UNATMO	4.7.9	The FI should assess whether this failure provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.

[17] The same principle applies to the verification of address for a direct customer; an example of a reasonable timeframe being 90 working days.

	4.7.10	Wherever possible, when terminating a relationship where funds or other assets have been received, the FI should return the funds or assets to the source from which they were received. In general, this means that the funds or assets should be returned to the customer/account holder but this may not always be possible.
	4.7.11	FIs must guard against the risk of ML/TF since this is a possible means by which funds can be "transformed", e.g. from cash into a cashier order. Where the customer requests that money or other assets be transferred to third parties, the FI should assess whether this provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.
Keeping customer information up-to-date		
s.5(1)(a), Sch. 2	4.7.12	Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); however, FIs should take steps from time to time to ensure that the customer information that has been obtained for the purposes of complying with the requirements of sections 2 and 3 of Schedule 2 are up-to-date and relevant. To achieve this, an FI should undertake periodic reviews of existing records of customers. An appropriate time to do so is upon certain trigger events. These include: (a) when a significant transaction[18] is to take place; (b) when a material change occurs in the way the customer's account is operated[19]; (c) when the FIs customer documentation standards change substantially; or (d) when the FI is aware that it lacks sufficient information about the customer concerned. In all cases, the factors determining the period of review or what constitutes a trigger event should be clearly defined in the FIs' policies and procedures.

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

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

	4.7.12a	*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;* *(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.*
	4.7.13	All high-risk customers (excluding dormant accounts) should be subject to a minimum of an annual review, and more frequently if deemed necessary by the FI, of their profile to ensure the CDD information retained remains up-to-date and relevant. FIs should however clearly define what constitutes a dormant account in their policies and procedures.

4.8 Natural persons		
Identification		
s.2, Sch. 2	4.8.1	FIs should collect the following identification information in respect of personal customers who need to be identified: (a) full name; (b) date of birth; (c) nationality; and (d) identity document type and number.
Verification (Hong Kong residents)		
s.2(1)(a), Sch. 2	4.8.2	For Hong Kong permanent residents, FIs should verify an individual's name, date of birth and identity card number by reference to their Hong Kong identity card. FIs should retain a copy of the individual's identity card.
	4.8.3	For children born in Hong Kong who are under the age of 12 and not in possession of a valid travel document or Hong Kong identity card, the child's identity should be verified by reference to their Hong Kong birth certificate. Whenever establishing business relationships with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should be recorded and verified in accordance with the above requirements.
	4.8.4	For non-permanent residents, FIs should verify an individual's name, date of birth, nationality and travel document number and type by reference to a valid travel document (e.g. an unexpired international passport). In this respect the FI should retain a copy of the "biodata" page which contains the bearer's photograph and biographical details. Alternatively, FIs may verify the individual's name, date of birth, identity card number by reference to their Hong Kong identity card and the individual's nationality by reference to: (a) a valid travel document; (b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph; or (c) any government or state-issued document which certifies nationality. FIs should retain a copy of the above documents.

Verification (non-residents)		
s.2(1)(a), Sch. 2	4.8.5	For non-residents who are physically present in Hong Kong for verification purposes, FIs should verify an individual's name, date of birth, nationality and travel document number and type by reference to a valid travel document (e.g. an unexpired international passport). In this respect the FI should retain a copy of the "biodata" page which contains the bearer's photograph and biographical details.
s.2(1)(a), Sch. 2	4.8.6	For non-residents who are not physically present in Hong Kong for verification purposes, FIs should verify the individual's identity, including name, date of birth, nationality, identity or travel document number and type by reference to: (a) a valid travel document; (b) a relevant national (i.e. government or state-issued) identity card bearing the individual's photograph; (c) a valid national driving license bearing the individual's photograph; or (d) any applicable alternatives mentioned in Appendix A.
s.9, Sch. 2	4.8.7	In respect of paragraph 4.8.6 above, where a customer has not been physically present for identification purposes, an FI must also carry out the measures at section 9 of Schedule 2, with reference to the guidance provided at paragraphs 4.12.
Address identification and verification		
	4.8.8	An FI should obtain and verify the residential address (and permanent address if different) of a direct customer with whom it establishes a business relationship as this is useful for verifying an individual's identity and background.
	4.8.9	For avoidance of doubt, it is the trustee of the trust who will enter into a business relationship or carry out a transaction on behalf of the trust and who will be considered to be the customer. The address of the trustee in a direct customer relationship should therefore always be verified.
	4.8.10	Methods for verifying residential addresses may include obtaining[20]: (a) a recent utility bill issued within the last 3 months; (b) recent correspondence from a Government department or agency

[20] The examples provided are not exhaustive.

		(i.e. issued within the last 3 months); (c) a statement, issued by an authorized institution, a licensed corporation or an authorized insurer within the last 3 months; (d) a record of a visit to the residential address by the FI; (e) an acknowledgement of receipt duly signed by the customer in response to a letter sent by the FI to the address provided by the customer; (f) a letter from an immediate family member at which the individual resides confirming that the applicant lives at that address in Hong Kong, setting out the relationship between the applicant and the immediate family member, together with evidence that the immediate family member resides at the same address (for persons such as students and housewives who are unable to provide proof of address of their own name); (g) mobile phone or pay TV statement (sent to the address provided by the customer) issued within the last 3 months; (h) a letter from a Hong Kong nursing or residential home for the elderly or disabled, which an FI is satisfied that it can place reliance on, confirming the residence of the applicant; (i) a letter from a Hong Kong university or college, which an FI is satisfied that it can place reliance on, that confirms residence at a stated address; (j) a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department; (k) a current Hong Kong domestic helper employment contract stamped by an appropriate Consulate (the name of the employer should correspond with the applicant's visa endorsement in their passport); (l) a letter from a Hong Kong employer together with proof of employment, which an FI is satisfied that it can place reliance on and that confirms residence at a stated address in Hong Kong; (m) a lawyer's confirmation of property purchase, or legal document recognising title to property; and (n) for non-Hong Kong residents, a government-issued photographic driving license or national identity card containing the current residential address or bank statements issued by a bank in an equivalent jurisdiction where the FI is satisfied that the address has been verified.
	4.8.11	It is conceivable that FIs may not always be able to adopt any of the suggested methods in the paragraph above. Examples include countries without postal deliveries and virtually no street addresses, where residents rely upon post office boxes or their employers for the delivery

		of mail. Some customers may simply be unable to produce evidence of address to the standard outlined above. In such circumstances FIs may, on a risk sensitive basis, adopt a common sense approach by adopting alternative methods such as obtaining a letter from a director or manager of a verified known overseas employer that confirms residence at a stated overseas address (or provides detailed directions to locate a place of residence). There may also be circumstances where a customer's address is a temporary accommodation and where normal address verification documents are not available. For example, an expatriate on a short-term contract. FIs should adopt flexible procedures to obtain verification by other means, e.g. copy of contract of employment, or bank's or employer's written confirmation. FIs should exercise a degree of flexibility under special circumstances (e.g. where a customer is homeless). For the avoidance of doubt, a post office box address is not sufficient for persons residing in Hong Kong or corporate customers registered and/or operating in Hong Kong.
Other considerations		
	4.8.12	The standard identification requirement is likely to be sufficient for most situations. If, however, the customer, or the product or service, is assessed to present a higher ML/TF risk because of the nature of the customer, his business, his location, or because of the product features, etc., the FI should consider whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.
	4.8.13	Appendix A contains a list of documents recognised by the RAs as independent and reliable sources for identity verification purposes.
4.9 Legal persons and trusts		
General		
	4.9.1	For legal persons, the principal requirement is to look behind the customer to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets. FIs would normally pay particular attention to persons who exercise ultimate control over the management of the customer.
s.2(1)(b), Sch. 2	4.9.2	In deciding who the beneficial owner is in relation to a legal person where the customer is not a natural person, the FI's objective is to know who has ownership or control over the legal person which relates to the relationship, or who constitutes the controlling mind and management

		of any legal entity involved in the funds. Verifying the identity of the beneficial owner(s) should be carried out using reasonable measures based on a risk-based approach, following the guidance in Chapter 3.
	4.9.3	Where the owner is another legal person or trust, the objective is to undertake reasonable measures to look behind that legal person or trust and to verify the identity of beneficial owners. What constitutes control for this purpose will depend on the nature of the institution, and may vest in those who are mandated to manage funds, accounts or investments without requiring further authorisation.
s.2(1)(b), Sch. 2	4.9.4	For a customer other than a natural person, FIs should ensure that they fully understand the customer's legal form, structure and ownership, and should additionally obtain information on the nature of its business, and the reasons for seeking the product or service unless the reasons are obvious.
s.5(1)(a) & s.6, Sch. 2	4.9.5	FIs should conduct reviews from time to time to ensure the customer information held is up-to-date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.
	4.9.6	Many entities operate internet websites, which contain information about the entity. FIs should bear in mind that this information, although helpful in providing much of the materials that an FI might need in relation to the customer, its management and business, may not be independently verified.
Corporation		
Identification information		
	4.9.7	The information below should be obtained as a standard requirement; thereafter, on the basis of the ML/TF risk, an FI should decide whether further verification of identity is required and if so the extent of that further verification. The FI should also decide whether additional information in respect of the corporation, its operation and the individuals behind it should be obtained. An FI should obtain and verify the following information in relation to a customer which is a corporation: (a) full name; (b) date and place of incorporation;

		(c) registration or incorporation number; and (d) registered office address in the place of incorporation. If the business address of the customer is different from the registered office address in (d) above, the FI should obtain information on the business address and verify as far as practicable.
	4.9.8	In the course of verifying the customer's information mentioned in paragraph 4.9.7, an FI should also obtain the following information[21]: (a) a copy of the certificate of incorporation and business registration (where applicable); (b) a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind the company; and (c) details of the ownership and structure control of the company, e.g. an ownership chart. For avoidance of doubt, this requirement does not apply in respect of a company falling within section 4(3) of Schedule 2.
	4.9.9	An FI should[22] record the names of all directors and verify the identity of directors on a risk-based approach.
	4.9.10	FIs should: (a) confirm the company is still registered and has not been dissolved, wound up, suspended or struck off; (b) independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation; and (c) verify the company's registered office address in the place of incorporation.
	4.9.11	The FI should verify the information in paragraph 4.9.10 from: for a locally incorporated company: (a) a search of file at the Hong Kong Company Registry and obtain a

[21] Examples given are not exhaustive.

[22] The FI may, of course, be already be required to identify a particular director if the director acts as a beneficial owner or a person purporting to act on behalf of the customer (e.g. account signatories). (see paragraphs 4.3 and 4.4)

		company report[23]; for a company incorporated overseas: (b) a similar company search enquiry of the registry in the place of incorporation and obtain a company report[23]; (c) a certificate of incumbency[24] or equivalent issued by the company's registered agent in the place of incorporation; or (d) a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction verifying that the information at paragraph 4.9.10, contained in the said document, is correct and accurate. For avoidance of doubt, this requirement does not apply in respect of a company falling within section 4(3) of Schedule 2.
	4.9.12	If the FI has obtained a company search report pursuant to paragraph 4.9.11 which contains information such as certificate of incorporation, company's memorandum and articles of association, etc, the FI is not required to obtain the same information again from the customer pursuant to paragraph 4.9.8.
Beneficial owners		
s.1, Sch. 2	4.9.13	The AMLO defines beneficial owner in relation to a corporation as: (i) an individual who – (a) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation; (b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or (c) exercises ultimate control over the management of the corporation; or (ii) if the corporation is acting on behalf of another person, means the other person.

[23] Alternatively, the FI may obtain from the customer a certified true copy of a company search report certified by a company registry or professional third party. The company search report should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the report to be self-certified by the customer.

[24] FIs may accept a certified true copy of a certificate of incumbency certified by a professional third party. The certificate of incumbency should have been issued within the last 6 months. For the avoidance of doubt, it is not sufficient for the certificate to be self-certified by the customer.

	4.9.14	An FI should identify and record the identity of all beneficial owners, and take reasonable measures to verify the identity of: (a) all shareholders holding more than 25% of the voting rights or share capital; (b) any individual who exercises ultimate control over the management of the corporation; and (c) any person on whose behalf the customer is acting.
	4.9.15	For companies with multiple layers in their ownership structures, an FI should ensure that it has an understanding of the ownership and control structure of the company. The intermediate layers of the company should be fully identified. The manner in which this information is collected should be determined by the FI, for example by obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk sensitive basis but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed). The objective should always be to follow the chain of ownership to the individuals who are the ultimate beneficial owners of the direct customer of the FI and verify the identity of those individuals.
	4.9.16	FIs need not, as a matter of routine, verify the details of the intermediate companies in the ownership structure of a company. Complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to ensure that the FI is satisfied on reasonable grounds as to the identity of the beneficial owners.
	4.9.17	The need to verify the intermediate corporate layers of the ownership structure of a company will therefore depend upon the FI's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the FI to consider if it has taken adequate measures to identify the beneficial owners.
	4.9.18	Where the ownership is dispersed, the FI should concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.

Partnerships and unincorporated bodies		
	4.9.19	Partnerships and unincorporated bodies, although principally operated by individuals or groups of individuals, are different from individuals, in that there is an underlying business. This business is likely to have a different ML/TF risk profile from that of an individual.
s.1, Sch. 2	4.9.20	The AMLO defines beneficial owner, in relation to a partnership as: (i) an individual who (a) is entitled to or controls, directly or indirectly, more than a 25 % share of the capital or profits of the partnership; (b) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or (c) exercises ultimate control over the management of the partnership; or (ii) if the partnership is acting on behalf of another person, means the other person.
s.1, Sch. 2	4.9.21	In relation to an unincorporated body other than a partnership, beneficial owner: (i) means an individual who ultimately owns or controls the unincorporated body; or (ii) if the unincorporated body is acting on behalf of another person, means the other person.
	4.9.22	The FI should obtain the following information in relation to the partnership or unincorporated body: (a) the full name; (b) the business address; and (c) the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control more than 25% of its capital or profits, or of its voting rights. In cases where a partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.
	4.9.23	The FI's obligation is to verify the identity of the customer using evidence from a reliable and independent source. Where partnerships

		or unincorporated bodies are well-known, reputable organisations, with long histories in their industries, and with substantial public information about them, their partners and controllers, confirmation of the customer's membership of a relevant professional or trade association is likely to be sufficient to provide such reliable and independent evidence of the identity of the customer. This does not remove the need to take reasonable measures to verify the identity of the beneficial owners[25] of the partnerships or unincorporated bodies.
	4.9.24	Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners and controllers. In verifying the identity of such customers, FIs should primarily have regard to the number of partners and controllers. Where these are relatively few, the customer should be treated as a collection of individuals; where numbers are larger, the FI should decide whether it should continue to regard the customer as a collection of individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either case, FIs should obtain the partnership deed (or other evidence in the case of sole traders or other unincorporated bodies), to satisfy themselves that the entity exists, unless an entry in an appropriate national register may be checked.
	4.9.25	In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, an FI should satisfy itself as to the legitimate purpose of the organisation, e.g. by requesting sight of the constitution.
Trusts		
General		
	4.9.26	A trust does not possess a separate legal personality. It cannot form business relationships or carry out occasional transactions itself. It is the trustee who enters into a business relationship or carries out occasional transactions on behalf of the trust and who is considered to be the customer (i.e. the trustee is acting on behalf of a third party – the trust and the individuals concerned with the trust).
s.1, Sch. 2	4.9.27	The AMLO defines the beneficial owner, in relation to a trust as: (i) an individual who is entitled to a vested interest in more than 25% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible

[25] Reference should be made to paragraph 4.3.1.

		or not; (ii) the settlor of the trust; (iii) a protector or enforcer of the trust; or (iv) an individual who has ultimate control over the trust.
	4.9.28	FIs should collect the following identification information in respect of a trust on whose behalf the trustee (i.e. the customer) is acting: (a) the name of the trust; (b) date of establishment/settlement; (c) the jurisdiction whose laws govern the arrangement, as set out in the trust instrument; (d) the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organization number); (e) identification information of trustee(s) - in line with guidance for individuals or corporations; (f) identification information of settlor(s) and any protector(s) or enforcers in line with the guidance for individuals/corporations; and (g) identification information of known beneficiaries [26]. Known beneficiaries mean those persons or that class of persons who can, from the terms of the trust instrument, be identified as having a reasonable expectation of benefiting from the trust capital or income.
Verifying the trust		
	4.9.29	An FI must verify the name and date of establishment of a trust and should obtain appropriate evidence to verify the existence, legal form and parties to it, i.e. trustee, settlor, protector, beneficiary, etc. The beneficiaries should be identified as far as possible where defined. If the beneficiaries are yet to be determined, the FI should concentrate on the identification of the settlor and/or the class of persons in whose interest the trust is set up. The most direct method of satisfying this requirement is to review the appropriate parts of the trust deed. Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/TF risk, may include: (a) reviewing a copy of the trust instrument and retaining a redacted copy;

[26] With reference to paragraph 4.9.27(i)

		(b) by reference to an appropriate register[27] in the relevant country of establishment; (c) a written confirmation from a trustee acting in a professional capacity[28]; (d) a written confirmation from a lawyer who has reviewed the relevant instrument; or (e) for trusts that are managed by the trust companies which are subsidiaries (or affiliate companies) of an FI, that FI may rely on a written confirmation from its trust subsidiaries (or trust affiliate companies). For the avoidance of doubt, reasonable measures are still required to be taken to verify[29] the actual identity of the individual parties (i.e. trustee, settlor, protector, beneficiary, etc.).
	4.9.30	Where only a class of beneficiaries is available for identification, the FI should ascertain and name the scope of the class (e.g. children of a named individual).
	4.9.31	Particular care should be taken in relation to trusts created in jurisdictions where there is no money laundering legislation similar to Hong Kong.
Other considerations		
	4.9.32	Appendix A contains a list of documents recognised by the RAs as independent and reliable sources for identity verification purposes.
4.10 Simplified customer due diligence (SDD)		
General		
	4.10.1	The AMLO defines what CDD measures are and also prescribes the circumstances in which an FI must carry out CDD. SDD means that application of full CDD measures is not required. In practice, this means that FIs are not required to identify and verify the beneficial owner[30]. However, other aspects of CDD must be undertaken and it is

[27] In determining whether a register is appropriate, regard should be had 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.

[28] "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).

[29] Reference should be made to paragraphs 4.3.1 and 4.9.27.

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

		still necessary to conduct ongoing monitoring of the business relationship. FIs must have reasonable grounds to support the use of SDD and may have to demonstrate these grounds to the relevant RA.
s.3(1)(d) & (e), s.4(1), (3), (5) & (6), Sch. 2	4.10.2	Nonetheless, SDD must not be applied when the FI suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding when the customer, the product, and account type falls within paragraphs 4.10.3, 4.10.15 and 4.10.17 below.
s.4(3), Sch. 2	4.10.3	The AMLO defines customers to whom SDD may be applied as follows: (a) an FI as defined in the AMLO; (b) an institution that- (i) is incorporated or established in an equivalent jurisdiction (see paragraphs 4.20); (ii) carries on a business similar to that carried on by an FI; (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs; (c) a corporation listed on any stock exchange ("listed company"); (d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is- (i) an FI; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that- i. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and ii. is supervised for compliance with those requirements. (e) the Government or any public body in Hong Kong; or (f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.4(2), Sch. 2	4.10.4	If a customer not falling within section 4(3) of Schedule 2 has in its ownership chain an entity that falls within that section, the FI is not

		required to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship with or carrying out an occasional transaction for the customer. However, FIs should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity.
s.2(1)(a), (c) & (d), Sch. 2	4.10.5	For avoidance of doubt, the FI must still: (a) identify the customer and verify[31] the customer's identity; (b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with the FI; and (c) if a person purports to act on behalf of the customer, (i) identify the person and take reasonable measures to verify the person's identity; and (ii) verify the person's authority to act on behalf of the customer, in accordance with the relevant requirements stipulated in this Guideline.
<u>Local and foreign financial institution</u>		
s.4(3)(a) & (b), Sch. 2	4.10.6	FIs may apply SDD to a customer that is an FI as defined in the AMLO, or an institution that carries on a business similar to that carried on by an FI and meets the criteria set out in section 4(3)(b) of Schedule 2. If the customer does not meet the criteria, the FI must carry out all the CDD measures set out in section 2 of Schedule 2. FIs may apply SDD to a customer that is an FI as defined in the AMLO that opens an account: (a) in the name of a nominee company for holding fund units on behalf of the second-mentioned FI or its underlying customers; or (b) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle and the underlying investors have no control over the management of the investment vehicle's assets; provided that the second-mentioned FI: (i) has conducted CDD:

[31] For FIs and listed companies, please refer to paragraphs 4.10.7 and 4.10.8 respectively.

		(A) in the case where the nominee company holds fund units on behalf of the second-mentioned FI or the second-mentioned FI's underlying customers, on its underlying customers; or (B) in the case where the second-mentioned FI acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle pursuant to the provisions of the AMLO; and (ii) is authorized to operate the account as evidenced by contractual document or agreement.
	4.10.7	For ascertaining whether the institution meets the criteria set out in section 4(3)(a) & (b) of Schedule 2, it will generally be sufficient for an FI to verify that the institution is on the list of authorized (and supervised) FIs in the jurisdiction concerned.
Listed company		
s.4(3)(c), Sch. 2	4.10.8	FIs may perform SDD in respect of a corporate customer listed on a stock exchange[32]. This means FIs need not identify the beneficial owners of the listed company. In such cases, it will be generally sufficient for an FI to obtain proof of listed status on a stock exchange. In all other cases, FIs should follow the CDD requirements for a legal person set out in paragraphs 4.9 of this Guideline.
Investment vehicle		
s.4(3)(d), Sch. 2	4.10.9	FIs may apply SDD to a customer that is an investment vehicle if the FI is able to ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2.
	4.10.10	An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity.
	4.10.11	An investment vehicle whether or not responsible for carrying out CDD measures on the underlying investors under governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment

[32] Reference should be made to paragraphs 4.15.

		vehicle[33] or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2, an FI may apply SDD to that investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the CDD (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in the Schedule 2.
	4.10.12	For the avoidance of doubt, if neither the investment vehicle nor appointed institution fall within any of the categories of institution set out in section 4(3)(d) of Schedule 2, the FI must identify any investor owning or controlling more than 25% interest of the investment vehicle. The FI may adopt a risk-based approach in determining if 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. In making the risk-based determination, the FI should take into consideration whether the investment vehicle is being operated for a small, specific group of persons. Where the FI accepts such a representation, this should be documented, retained, and subject to periodic review. Where investors owning or controlling more than 25% interest are identified, the FI must take reasonable measures to verify their identity itself.
Government and public body		
s.4(3)(e) & (f), Sch. 2	4.10.13	FIs may apply SDD to a customer that is the Hong Kong government, any public bodies in Hong Kong, the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.
s.1, Sch. 2	4.10.14	Public body includes: (a) any executive, legislative, municipal or urban council; (b) any Government department or undertaking; (c) any local or public authority or undertaking; (d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and (e) any board, commission, committee or other body that has power to

[33] 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.

		act in a public capacity under or for the purposes of any enactment.
SDD in relation to specific products		
s.4(4) & (5), Sch. 2	4.10.15	FIs may apply SDD in relation to a customer if the FI has reasonable grounds to believe that the transaction conducted by the customer relates to any one of the following products: (a) a provident, pension, retirement or superannuation scheme (however described) that provides retirement benefits to employees, where contributions to the scheme are made by way of deduction from income from employment and the scheme rules do not permit the assignment of a member's interest under the scheme; (b) an insurance policy for the purposes of a provident, pension, retirement or superannuation scheme (however described) that does not contain a surrender clause and cannot be used as a collateral; or (c) a life insurance policy in respect of which: (i) an annual premium of no more than $8,000 or an equivalent amount in any other currency is payable; or (ii) a single premium of no more than $20,000 or an equivalent amount in any other currency is payable.
	4.10.16	For the purpose of item (a) of paragraph 4.10.15, FIs may generally treat the employer as the customer and apply SDD on the employer. Where FIs have a business relationship with the employees, it should identify and verify the identities of the employees in accordance with the requirements set out in paragraphs 4.8.
Solicitor's client accounts		
s.4(6), Sch. 2	4.10.17	If a customer of an FI is a solicitor or a firm of solicitors, the FI is not required to identify 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.
	4.10.18	In addition to performing the normal CDD on the customer, when opening a client account for a solicitor or a firm of solicitors, FIs should establish the proposed use of the account, i.e. whether to hold co-mingled client funds or the funds of a specific client.

	4.10.19	FI should obtain evidence to satisfy that the solicitor is authorized to practise in Hong Kong or in an equivalent jurisdiction. FIs may assume that the solicitor has reliable and proper systems in place to identify each client and allocate the funds to the underlying client and apply SDD unless they become aware of any adverse information (e.g. adverse publicity or reprimand by the Law Society) to the contrary.
	4.10.20	If a client account is opened on behalf of a single client or there are sub-accounts for each individual client where funds are not co-mingled at the FI, the FI should establish the identity of the underlying client(s) in addition to that of the solicitor opening the account.
4.11 High-risk situations		
s.15, Sch. 2	4.11.1	Section 15 of Schedule 2 specifies that an FI must, in any situation that by its nature presents a higher risk of ML/TF, take additional measures to mitigate the risk of ML/TF. Additional measures[34] or EDD should be taken to mitigate the ML/TF risk involved, which for illustration purposes, may include: (a) obtaining additional information on the customer (e.g. connected parties[35], accounts or relationships) and updating more regularly the customer profile including the identification data; (b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity), the source of wealth and source of funds; (c) obtaining the approval of senior management to commence or continue the relationship; and (d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination. For avoidance of doubt, all high-risk customers should be subject to a minimum annual review with reference to paragraph 4.7.13.
4.12 Customer not physically present for identification purposes		
	4.12.1	FIs must apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for

[34] Additional measures should be documented in the FI's policies and procedures.
[35] Consideration might be given to obtaining, and taking reasonable measures to verify, the addresses of directors and account signatories.

		interview[36]. Where a customer has not been physically present for identification purposes, FIs will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, there are increased risks.
s.5(3)(a) & s.9, Sch. 2	4.12.2	The AMLO requires an FI to take additional measures to compensate for any risk associated with customers not physically present for identification purposes. If a customer has not been physically present for identification purposes, the FI must carry out at least one of the following measures to mitigate the risks posed: (a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 but not previously used for the purposes of verification of the customer's identity under that section; (b) taking supplementary measures to verify information relating to the customer that has been obtained by the FI; (c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 and is supervised for compliance with those requirements by a banking regulator in that jurisdiction. Consideration should be given on the basis of the ML/TF risk to obtaining copies of documents that have been certified by a suitable certifier.
Suitable certifiers and the certification procedure		
	4.12.3	Use of an independent suitable certifier guards against the risk that documentation provided does not correspond to the customer whose identity is being verified. However, for certification to be effective, the certifier will need to have seen the original documentation.
	4.12.4	Suitable persons to certify verification of identity documents may include: (a) an intermediary specified in section 18(3) of Schedule 2; (b) a member of the judiciary in an equivalent jurisdiction; (c) an officer of an embassy, consulate or high commission of the

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

		country of issue of documentary verification of identity; and (d) a Justice of the Peace.
	4.12.5	The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it. The certifier must state that it is a true copy of the original (or words to similar effect).
	4.12.6	FIs remain liable for failure to carry out prescribed CDD and therefore must exercise caution when considering accepting certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. In any circumstances where an FI is unsure of the authenticity of certified documents, or that the documents relate to the customer, FIs should take additional measures to mitigate the ML/TF risk.
4.13 Politically exposed persons (PEPs)		
General		
s.1 & s.10, Sch. 2	4.13.1	Much international attention has been paid in recent years to the risk associated with providing financial and business services to those with a prominent political profile or holding senior public office. However, PEP status itself does not automatically mean that the individuals are corrupt or that they have been incriminated in any corruption.
	4.13.2	However, their office and position may render PEPs vulnerable to corruption. The risks increase when the person concerned is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such countries do not have adequate AML/CFT standards.
s.15, Sch. 2	4.13.3	While the statutory definition of PEPs in the AMLO (see paragraph 4.13.5 below) only includes individuals entrusted with prominent public function in a place outside the People's Republic of China[37], domestic PEPs may also present, by virtue of the positions they hold, a high risk situation where EDD should be applied. FIs should therefore adopt a risk-based approach to determining whether to apply the measures in paragraph 4.13.11 below in respect of domestic PEPs.

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

s.1, s.15 & s.5(3)(c), Sch. 2	4.13.4	The statutory definition does not automatically exclude sub-national political figures. Corruption by heads of regional governments, regional government ministers and large city mayors is no less serious as sub-national figures in some jurisdictions may have access to substantial funds. Where FIs identify a customer as a sub-national figure holding a prominent public function, they should apply appropriate EDD. This also applies to domestic sub-national figures assessed by the FI to pose a higher risk. In determining what constitutes a prominent public function, FIs should consider factors such as persons with significant influence in general, significant influence over or control of public procurement or state owned enterprises, etc.
<u>(Foreign) Politically exposed person</u>		
s.1, Sch. 2	4.13.5	A politically exposed person is defined in the AMLO as: (a) an individual who is or has been entrusted with a prominent public function in a place outside the People's Republic of China and (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 4.13.6).
s.1, Sch. 2	4.13.6	The AMLO defines a close associate as: (a) an individual who has close business relations with a person falling under paragraph 4.13.5(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph 4.13.5(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 4.13.5(a) above.
	4.13.7	FIs that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face reputational and legal risks, including the possibility of criminal charges for having assisted in laundering the proceeds of crime.

	4.13.8	FIs can reduce risk by conducting EDD at the outset of the business relationship and ongoing monitoring where they know or suspect that the business relationship is with a PEP.
s.19(1), Sch. 2	4.13.9	FIs must establish and maintain effective procedures (for example making reference to publicly available information and/or screening against commercially available databases) for determining whether a customer or a beneficial owner of a customer is a PEP. These procedures should extend to the connected parties of the customer using a risk-based approach.
	4.13.10	FIs may use publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption). FIs should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.
s.5(3)(b) & s.10, Sch. 2	4.13.11	When FIs know that a particular customer or beneficial owner is a 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 PEP, apply all the following EDD measures: (a) obtaining approval from its senior management; (b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and (c) applying enhanced monitoring to the relationship in accordance with the assessed risks.
	4.13.12	It is for an FI to decide which measures it deems reasonable, in accordance with its assessment of the risks, to establish the source of funds and source of wealth. In practical terms, this will often amount to obtaining information from the PEP and verifying it against publicly available information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. FIs should however note that not

		all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. FIs should also be aware that some jurisdictions impose restrictions on their PEP's ability to hold foreign bank accounts or to hold other office or paid employment.
Senior management approval		
	4.13.13	While the AMLO is silent on the level of senior management who may approve the establishment or continuation of the relationship, the approval process should take into account the advice of the FI's CO. The more potentially sensitive the PEP, the higher the approval process should be escalated.
Domestic politically exposed persons		
	4.13.14	For the purposes of this Guideline, a domestic PEP is defined as: (a) an individual who is or has been entrusted with a prominent public function in a place within the People's Republic of China 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 4.13.6).
	4.13.15	FIs should take reasonable measures to determine whether an individual is a domestic PEP.
s.5(3)(c) & s.15, Sch. 2	4.13.16	If an individual is known to be a domestic PEP, the FI should perform a risk assessment to determine whether the individual poses a higher risk of ML/TF. Domestic PEPs status in itself does not automatically confer higher risk. In any situation that the FI assesses to present a higher risk of ML/TF, it should apply the EDD and monitoring specified in paragraph 4.11.1.
	4.13.17	FIs should retain a copy of the assessment for RAs, other authorities and auditors and should review the assessment whenever concerns as to the activities of the individual arise.

Periodic reviews		
	4.13.18	For foreign PEPs and domestic PEPs assessed to present a higher risk, they should be subject to a minimum annual review. FIs should review CDD information to ensure that it remains up-to-date and relevant.
4.14 Bearer shares		
	4.14.1	Bearer shares are an equity security that is wholly owned by whoever holds the physical stock certificate. The issuing corporate does not register the owner of the stock or track transfers of ownership. Transferring the ownership of the stock involves only delivering the physical document. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded. Due to the higher ML/TF risks associated with bearer shares the FATF requires countries that have legal persons able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering.
s.15, Sch. 2	4.14.2	To reduce the opportunity for bearer shares to be used to obscure information on beneficial ownership, FIs must take additional measures in the case of companies with capital in the form of bearer shares, as it is often difficult to identify the beneficial owner(s). FIs should adopt procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified whenever there is a change of holder or beneficial owner.
	4.14.3	Where bearer shares have been deposited with an authorized/registered custodian, FIs should seek independent evidence of this, for example confirmation from the registered agent that an authorized/registered custodian holds the bearer shares, the identity of the authorized/registered custodian and the name and address of the person who has the right to those entitlements carried by the share. As part of the FI's ongoing periodic review, it should obtain evidence to confirm the authorized/registered custodian of the bearer shares.
	4.14.4	Where the shares are not deposited with an authorized/registered custodian, the FI should obtain declarations prior to account opening and annually thereafter from each beneficial owner of such shares. FIs should also require the customer to notify it immediately of any changes in the ownership of the shares.
4.15 Jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise posing higher risk		
	4.15.1	FIs should give particular attention to, and exercise extra care in respect of:

		(a) business relationships and transactions with persons (including legal persons and other FIs) from or in jurisdictions that do not or insufficiently apply the FATF Recommendations; and (b) transactions and business connected with jurisdictions assessed as higher risk. Based on the FI's assessment of the risk in either case, the special requirements of section 15 of Schedule 2 may apply. In addition to ascertaining and documenting the business rationale for establishing a relationship, an FI should take reasonable measures to establish the source of funds of such customers.
	4.15.2	In determining which jurisdictions do not apply, or insufficiently apply the FATF Recommendations, or may otherwise pose a higher risk, FIs should consider, among other things: (a) circulars issued to FIs by RAs; (b) whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances where a jurisdiction is subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, the sanctions or measures may still be given credence by an FI because of the standing of the issuer and the nature of the measures; (c) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures; (d) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it; and (e) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity. "Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and

		should not be viewed as an automatic determination that something is of higher risk. An FI should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of ML/TF. If an FI incorporated in Hong Kong has operating units in such jurisdictions, care should be taken to ensure that effective controls on prevention of ML/TF are implemented in these units. In particular, the FI should ensure that the policies and procedures adopted in such overseas units are similar to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong.
4.16 Notice in writing from an RA		
s.15, Sch. 2	4.16.1	Where the requirement is called for by the FATF (which may include mandatory EDD or the application of countermeasures[38]) or in other circumstances independent of the FATF but also considered to be higher risk, RA may, through a notice in writing: (a) impose a general obligation on FIs to undertake EDD measures; or (b) require FIs to undertake specific countermeasures identified or described in the notice. The type of EDD/countermeasures would be proportionate to the nature of the risks and/or deficiencies.
4.17 Reliance on CDD performed by intermediaries		
General		
s.18, Sch. 2	4.17.1	An FI may rely upon an intermediary to perform any part of the CDD measures[39] specified in section 2 of Schedule 2, subject to the criteria set out in section 18 of Schedule 2. However, the ultimate responsibility for ensuring that CDD requirements are met remains with the FI.

[38] For jurisdictions with serious deficiencies in applying the FATF's Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of counter-measures.

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

		In a third-party reliance scenario, the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying FI, and would apply its own procedures to perform the CDD measures.
	4.17.1a	*Authorized insurers, reinsurers, appointed insurance agents and authorized insurance brokers all have the responsibility to comply with the requirements relating to CDD as set out in Schedule 2. However, insurance agents and brokers 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 appointed insurance agents, although such insurer remains liable for a failure to carry out that CDD measure. The insurer should be satisfied that its appointed agents have adequate procedures in place to prevent ML and TF, namely:* *(a) the CDD procedures of the agent should be as rigorous as those which the insurer would have conducted itself for the customer; and* *(b) the insurer is satisfied as to the reliability of the systems put in place by the agent to comply with the CDD requirements of Schedule 2.* *If a customer is introduced to an authorized insurer through an insurance broker, the insurer may rely on the broker to carry out any CDD measures pursuant to s. 18(1) of Schedule 2. In this case, paragraphs 4.17.3 to 4.17.7 are to be observed.*
	4.17.2	For the avoidance of doubt, reliance on intermediaries does not apply to: (a) outsourcing or agency relationships, in which the outsourced entity or agent applies the CDD measures on behalf of the FI, in accordance with the FI's procedures, and subject to the FI's control of effective implementation of these procedures by the outsourced entity or agent; and (b) business relationships, accounts or transactions between FIs for their customers.
s.18(1) & s.18(4)(b), Sch. 2	4.17.3	The FI must obtain written confirmation from the intermediary that: (a) it agrees to perform the role; and

		(b) it will provide without delay a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the FI upon request. The FI must ensure that the intermediary will, if requested by the FI within the period specified in the record-keeping requirements of AMLO, provide to the FI a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out that measure as soon as reasonably practicable after receiving the request.
s.18(4)(a), Sch. 2	4.17.4	An FI that carries out a CDD measure by means of an intermediary must immediately after the intermediary has carried out that measure, obtain from the intermediary the data or information that the intermediary has obtained in the course of carrying out that measure, but nothing in this paragraph requires the FI to obtain at the same time from the intermediary a copy of the document, or a record of the data or information, that is obtained by the intermediary in the course of carrying out that measure.
	4.17.5	Where these documents and records are kept by the intermediary, the FI should obtain an undertaking from the intermediary to keep all underlying CDD information throughout the continuance of the FI's business relationship with the customer and for at least five years beginning on the date on which the business relationship of a customer with the FI ends or until such time as may be specified by the RA. The FI should also obtain an undertaking from the intermediary to supply copies of all underlying CDD information in circumstances where the intermediary is about to cease trading or does not act as an intermediary for the FI anymore.
	4.17.6	An FI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay.
	4.17.7	Whenever an FI has doubts as to the reliability of the intermediary, it should take reasonable steps to review the intermediary's ability to perform its CDD duties. If the FI intends to terminate its relationship with the intermediary, it should immediately obtain all CDD information from the intermediary. If the FI has any doubts regarding the CDD measures carried out by the intermediary previously, the FI should perform the required CDD as soon as reasonably practicable.

Domestic intermediaries		
s.18(3)(a), (3)(b) & (7), Sch. 2	4.17.8	An FI may rely upon any one of the following domestic intermediaries, to perform any part of the CDD measures set out in section 2 of Schedule 2: (a) an FI that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker (intermediary FI); (b) an accounting professional meaning: (i) a certified public accountant or a certified public accountant (practising), as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); (ii) a corporate practice as defined by section 2(1) of the Professional Accountants Ordinance (Cap. 50); or (iii) a firm of certified public accountants (practising) registered under Part IV of the Professional Accountants Ordinance (Cap. 50); (c) an estate agent meaning: (i) a licensed estate agent as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); or (ii) a licensed salesperson as defined by section 2(1) of the Estate Agents Ordinance (Cap. 511); (d) a legal professional meaning: (i) a solicitor as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or (ii) a foreign lawyer as defined by section 2(1) of the Legal Practitioners Ordinance (Cap. 159); or (e) a trust or company service provider (TCSP) licensee meaning: (i) a person who holds a licence granted under section 53G or renewed under section 53K of the AMLO; or (ii) a deemed licensee as defined by section 53ZQ(5) of the AMLO, provided that in the case of an accounting professional, an estate agent, a legal professional or a TCSP licensee, the FI is satisfied that the domestic intermediary has adequate procedures in place to prevent ML/TF and is required to comply with the relevant requirements set out in Schedule 2 with respect to the customer[40].

[40] 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.

s.18(3)(a) & (3)(b), Sch. 2	4.17.9	An FI should take appropriate measures to ascertain if the domestic intermediary satisfies the criteria set out in paragraph 4.17.8, which may include: (a) where the domestic intermediary is an accounting professional, an estate agent, a legal professional or a TCSP licensee, ascertaining whether the domestic intermediary is required to comply with the relevant requirements set out in Schedule 2 with respect to the customer; (b) making enquiries concerning the domestic intermediary's stature or the extent to which any group AML/CFT standards are applied and audited; or (c) reviewing the AML/CFT policies and procedures of the domestic intermediary.
Overseas intermediaries		
18(3)(c), Sch. 2	4.17.10	An FI may rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction [41,42] 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 trust or company service provider; (v) a trust company carrying on trust business; and (vi) a person who carries on a business similar to that carried on by an estate agent; (b) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction; (c) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and (d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the RAs or the regulatory bodies (as may be applicable).

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

[42] Guidance on jurisdictional equivalence is provided in paragraphs 4.20.

	4.17.11	An FI should take appropriate measures to ascertain if the overseas intermediary satisfies the criteria set out in paragraph 4.17.10. Appropriate measures that should be taken to ascertain if the criterion set out in paragraph 4.17.10(c) is satisfied may include: (a) making enquiries concerning the overseas intermediary's stature or the extent to which any group's AML/CFT standards are applied and audited; or (b) reviewing the AML/CFT policies and procedures of the overseas intermediary.
Related foreign financial institutions as intermediaries		
s.18(3)(d), (3A) & (7), Sch. 2	4.17.12	An FI may also rely upon a related foreign financial institution (related foreign FI) to perform any part of the CDD measures set out in section 2 of Schedule 2, if the related foreign FI: (a) carries on, in a place outside Hong Kong, a business similar to that carried on by an intermediary FI; and falls within any of the following descriptions: (i) it is within the same group of companies as the FI; (ii) if the FI is incorporated in Hong Kong, it is a branch of the FI; (iii) if the FI is incorporated outside Hong Kong: (A) it is the head office of the FI; or (B) it is a branch of the head office of the FI; (b) is required under group policy: (i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2; and (ii) to implement programmes against ML/TF; and (c) is supervised for compliance with the requirements mentioned in paragraph (b) at a group level: (i) by an RA; or (ii) by an authority in an equivalent jurisdiction[43] that performs, in relation to the holding company or the head office of the FI, functions similar to those of an RA under the AMLO.

[43] Guidance on jurisdictional equivalence is provided in paragraphs 4.20.

s.18(3A) & (4)(c), Sch. 2	4.17.13	The group policy set out in paragraph 4.17.12(b) refers to a policy of the group of companies to which the FI belongs and the policy applies to the FI and the related foreign FI. The group policy should include CDD and record keeping requirements similar to the requirements imposed under Schedule 2 and a group-wide AML/CFT system[44] (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 FI should be satisfied that the related foreign FI is subject to regular and independent reviews over its ongoing compliance with the group policy conducted by any group-level compliance, audit or other similar AML/CFT functions.
s.18(3A), Sch. 2	4.17.14	The FI should be able to demonstrate that the implementation of the group policy is supervised at a group level by either an RA or an authority in an equivalent jurisdiction that performs functions similar to those of an RA under the AMLO, which practises group-wide supervision which extends to the related foreign FI.
4.18 Pre-existing customers		
Application of AMLO and guideline to pre-existing customers		
s.6, Sch. 2	4.18.1	FIs must perform the CDD measures prescribed in Schedule 2 and this Guideline in respect of pre-existing customers (with whom the business relationship was established before the AMLO came into effect on 1 April 2012), when: (a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the FI's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds; (b) a material change occurs in the way in which the customer's account is operated; (c) the FI suspects that the customer or the customer's account is involved in ML/TF; or (d) the FI doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.
	4.18.2	Trigger events may include the re-activation of a dormant account or a change in the beneficial ownership or control of the account but FIs

[44] Reference should be made to Chapter 2.

		will need to consider other trigger events specific to their own customers and business.
	4.18.2a	*Examples of trigger events after establishment of an insurance contract are provided in paragraph 4.7.12a.*
s.5, Sch. 2	4.18.3	FIs should note that requirements for ongoing monitoring under section 5 of Schedule 2 also apply to pre-existing customers (see Chapter 5).
4.19 Prohibition on anonymous accounts		
s.16, Sch. 2	4.19.1	FIs must not maintain anonymous accounts or accounts in fictitious names for any new or existing customer. Where numbered accounts exist, FIs must maintain them in such a way that full compliance can be achieved with the AMLO. FIs must properly identify and verify the identity of the customer in accordance with the Guideline. In all cases, whether the relationship involves numbered accounts or not, the customer identification and verification records must be available to the CO, other appropriate staff, RAs, other authorities and auditors upon appropriate authority.
4.20 Jurisdictional equivalence		
General		
s.4(3)(b)(i), s.4(3)(d)(iii), s.4(3)(f), s.9(c)(ii) s.18(3)(c), Sch. 2	4.20.1	Jurisdictional equivalence and the determination of equivalence is an important aspect in the application of CDD measures under the AMLO. For example, section 4 of Schedule 2 restricts the application of SDD to overseas institutions that carry on a business similar to that carried on by an FI and are incorporated or established in an equivalent jurisdiction.
	4.20.2	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		
	4.20.3	FIs may therefore be required to evaluate and determine for themselves which jurisdictions other than FATF members apply requirements similar to those imposed under Schedule 2 for jurisdictional equivalence purposes. When doing so an FI should document its assessment of the jurisdiction, which may include consideration of the following factors:

		(a) membership of a regional group of jurisdictions that admit as members only jurisdictions that have demonstrated a commitment to the fight against ML/TF, and which have an appropriate legal and regulatory regime to back up this commitment. Where a jurisdiction is a member of such a group, this may be taken into account as a supporting factor in the FI's assessment of whether the jurisdiction is likely to be "equivalent"; (b) mutual evaluation reports. Particular attention should be paid to assessments that have been undertaken by the FATF, FATF-style regional bodies, the International Monetary Fund and the World Bank. FIs should bear in mind that mutual evaluation reports are at a "point in time", and should be interpreted as such; (c) lists of jurisdictions published by the FATF with strategic AML/CFT deficiencies through the International Co-operation Review Group processes; (d) advisory circulars issued by RAs from time to time alerting FIs to such jurisdictions with poor AML/CFT controls; (e) lists of jurisdictions, entities and individuals that are involved, or that are alleged to be involved, in activities that cast doubt on their integrity in the AML/CFT area that are published by specialised national, international, non-governmental and commercial organisations. An example of such is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption; and (f) guidance provided at paragraphs 4.15 "Jurisdictions that do not or insufficiently apply the FATF's recommendations or otherwise posing a higher risk".
	4.20.4	The judgment on equivalence is one to be made by each FI in the light of the particular circumstances and senior management is accountable for this judgment. It is therefore important that the reasons for concluding that a particular jurisdiction is equivalent (other than those jurisdictions that are FATF members) are documented at the time the decision is made, and that the decision is made on up-to-date and relevant information. A record of the assessment performed and factors considered should be retained for regulatory scrutiny and periodically reviewed to ensure it remains up-to-date and valid.

Chapter 5 - ONGOING MONITORING		
General		
s.5(1), Sch. 2	5.1	Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CFT systems. It helps FIs to know their customers and to detect unusual or suspicious activities. An FI must continuously monitor its business relationship with a customer by: (a) reviewing from time to time documents, data and information relating to the customer and obtained pursuant to sections 2 and 3 of Schedule 2 to ensure that they are up-to-date and relevant[45]; (b) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that is being delivered; and (c) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.
	5.2	Failure to conduct ongoing monitoring could expose an FI to potential abuse by criminals, and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the FI's management.
	5.3	Possible characteristics FIs should consider monitoring include: (a) the nature and type of transactions (e.g. abnormal size or frequency); (b) the nature of a series of transactions (e.g. a number of cash deposits); (c) the amount of any transactions, paying particular attention to particularly substantial transactions; (d) the geographical origin/destination of a payment or receipt; and (e) the customer's normal activity or turnover.
	5.4	FIs should be vigilant for changes on the basis of the business relationship with the customer over time. These may include where:

[45] See paragraphs 4.7.12 and 4.7.13.

		(a) new products or services that pose higher risk are entered into; (b) new corporate or trust structures are created; (c) the stated activity or turnover of a customer changes or increases; or (d) the nature of transactions changes or their volume or size increases etc.
	5.5	Where the basis of the business relationship changes significantly, FIs should carry out further CDD procedures to ensure that the ML/TF risk involved and basis of the relationship are fully understood. Ongoing monitoring procedures must take account of the above changes.
	5.6	FIs should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU and should update the CDD information where appropriate; this will enable FIs to assess appropriate levels of ongoing review and monitoring.
Risk-based approach to monitoring		
	5.7	The extent of monitoring should be linked to the risk profile of the customer which has been determined through the risk assessment required in Chapter 3. To be most effective, resources should be targeted towards business relationships presenting a higher risk of ML/TF.
s.5(3), Sch. 2	5.8	FIs must take additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring. In monitoring high-risk situations, relevant considerations may include: (a) whether adequate procedures or management information systems are in place to provide relevant staff (e.g. CO, MLRO, front line staff, relationship managers and insurance agents) with timely information that might include, as a result of EDD or other additional measures undertaken, any information on any connected accounts or relationships; and (b) how to monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded.
<u>Methods and procedures</u>		
	5.9	When considering how best to monitor customer transactions and activities, an FI should take into account the following factors:

		(a) the size and complexity of its business; (b) its assessment of 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 (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) and transaction monitoring systems. Exception reports will help FI's stay apprised of operational activities.
s.5(1)(c), Sch. 2	5.10	Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, FIs should examine the background and purpose, including where appropriate the circumstances, of the transactions. The findings and outcomes of these examinations should be properly documented in writing and be available to assist the RAs, other competent authorities and auditors. Proper records of decisions made, by whom, and the rationale for them will help an FI demonstrate that it is handling unusual or suspicious activities appropriately.
s. 25A(5), DTROP & OSCO, s.12(5), UNATMO	5.11	Such examinations may include asking the customer questions, based on common sense, that a reasonable person would ask in the circumstances. Such enquiries, when conducted properly and in good faith, do not constitute tipping off *(see: <www.jfiu.gov.hk/en/str_ask.html>)*. These enquiries are directly linked to the CDD requirements, and reflect the importance of "knowing your customer" in detecting unusual or suspicious activities. Such enquiries and their results should be properly documented and be available to assist the RAs, other authorities and auditors. Where there is any suspicion, a report must be made to the JFIU.
	5.12	Where cash transactions (including deposits and withdrawals) and transfers to third parties are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, FIs must approach such situations with caution and make relevant further enquiries. Where the FI has been unable to satisfy itself that any cash transaction or third party transfer is reasonable, and therefore considers it suspicious, it should make a suspicious transaction report (STR) to the JFIU.

Chapter 6 – FINANCIAL SANCTIONS AND TERRORIST FINANCING		
Financial sanctions & proliferation financing		
	6.1	The obligations under the Hong Kong's financial sanctions regime apply to all persons, and not just FIs.
s.3(1), UNSO	6.2	The United Nations Sanctions Ordinance, Cap. 537 (UNSO) gives the Chief Executive the authority to make regulations to implement sanctions decided by the Security Council of the United Nations and to specify or designate relevant persons and entities.
	6.3	These sanctions normally prohibit making available or dealing with, directly or indirectly, any funds or economic resources for the benefit of or belonging to a designated party.
	6.4	RAs circulate to all FIs designations published in the government Gazette under the UNSO.
	6.5	While FIs will not normally have any obligation under Hong Kong law to have regard to lists issued by other organisations or authorities in other jurisdictions, an FI operating internationally will need to be aware of the scope and focus of relevant financial/trade sanctions regimes in those jurisdictions. Where these sanctions may affect their operations, FIs should consider what implications exist for their procedures, such as the consideration to monitor the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list issued by an overseas jurisdiction.
Applicable UNSO Regulation	6.6	The Chief Executive can licence exceptions to the prohibitions on making funds and economic resources available to a designated party under the UNSO. An FI seeking such a licence should write to the Commerce and Economic Development Bureau.
Terrorist financing		
	6.7	Terrorist financing generally refers to the carrying out of transactions involving property that are owned by terrorists, or that have been, or are intended to be, used to assist the commission of terrorist acts. This has not previously been explicitly covered under the money laundering regime where the focus is on the handling of criminal proceeds, i.e. the source of property is what matters. In terrorist financing, the focus is on the destination or use of property, which may have derived from legitimate sources.
UNSCR	6.8	The UN Security Council has passed United Nations Security Council

1373 (2001)		Resolution (UNSCR) 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UNSCRs regarding terrorism can be found at: www.un.org/sc/ctc/.
UNSCR 1267 (1999); 1390 (2002); 1617 (2005)	6.9	The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama bin Laden, Al-Qa'ida, and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1390 (2002) and 1617 (2005)). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.
	6.10	The United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO) was enacted in 2002 to give effect to the mandatory elements of UNSCR 1373 and the Special Recommendations of the FATF.
s. 6, UNATMO	6.11	The Secretary for Security (S for S) has the power to freeze suspected terrorist property and may direct that a person shall not deal with the frozen property except under the authority of a licence. Contraventions are subject to a maximum penalty of 7 years imprisonment and an unspecified fine.
	6.12	Section 6 of the UNATMO essentially confers the S for S an administrative power to freeze suspected terrorist property for a period of up to two years, during which time the authorities may apply to the court for an order to forfeit the property. This administrative freezing mechanism will enable the S for S to take freezing action upon receiving intelligence of suspected terrorist property in Hong Kong.
s.8 & 14, UNATMO	6.13	It is an offence for any person to make any property or financial services available, by any means, directly or indirectly, to or for the benefit of a terrorist or terrorist associate except under the authority of a licence granted by S for S. It is also an offence for any person to collect property or solicit financial (or related) services, by any means, directly or indirectly, for the benefit of a terrorist or terrorist associate. Contraventions are subject to a maximum sentence of 14 years imprisonment and an unspecified fine.
	6.14	Section 8 of the UNATMO does not affect a freeze per se; it prohibits a person from (i) making available, by any means, directly or indirectly,

		any property or financial services to or for the benefit of a person he knows or has reasonable grounds to suspect is a terrorist or terrorist associate, in the absence of a licence granted by S for S; and (ii) collecting property or soliciting financial (or related) services, by any means, directly or indirectly, for the benefit of a person he knows or has reasonable grounds to suspect is a terrorist or terrorist associate.
s.6(1), UNATMO	6.15	The S for S can licence exceptions to the prohibitions to enable frozen property and economic resources to be unfrozen and to allow payments to be made to or for the benefit of a designated party under the UNATMO. An FI seeking such a licence should write to the Security Bureau.
s.4(1), UNATMO	6.16	Where a person is designated by a Committee of the United Nations Security Council as a terrorist and his details are subsequently published in a notice under section 4 of the UNATMO in the Government gazette, RAs will circulate the designations to all FIs.
s.4, WMD(CPS)O	6.17	It is an offence under section 4 of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (WMD(CPS)O), Cap. 526, for a person to provide any services where he believes or suspects, on reasonable grounds, that those services may be connected to WMD proliferation. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.
	6.18	FIs may draw reference from a number of sources including relevant designation by overseas authorities, such as the designations made by the US Government under relevant Executive Orders. The RA may draw the FI's attention to such designations from time to time. All FIs will therefore need to ensure that they should have appropriate system to conduct checks against the relevant list for screening purposes and that this list is up-to-date.
Database maintenance and screening (customers and payments)		
	6.19	FIs should take measures to ensure compliance with the relevant regulations and legislation on terrorist financing. The legal obligations of FIs and those of its staff should be well understood and adequate guidance and training should be provided to the latter. FIs are required to establish policies and procedures for combating terrorist financing. The systems and mechanisms for identification of suspicious transactions should cover terrorist financing as well as money laundering.

	6.20	It is particularly vital that an FI should be able to identify and report transactions with terrorist suspects and designated parties. To this end, the FI should ensure that it maintains a database of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it. Alternatively, an FI may make arrangements to access to such a database maintained by third party service providers.
	6.21	FIs should ensure that the relevant designations are included in the database. Such database should, in particular, include the lists published in the Gazette and those designated under the US Executive Order 13224. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.
	6.22	Comprehensive ongoing screening of an FI's complete customer base is a fundamental internal control to prevent terrorist financing and sanction violations, and should be achieved by: (a) screening customers against current terrorist and sanction designations at the establishment of the relationship; and (b) thereafter, as soon as practicable after new terrorist and sanction designations are published by the RAs that these new designations, screening against their entire client base.
	6.23	FIs need to have some means of screening payment instructions to ensure that proposed payments to designated parties are not made. FIs should be particularly alert for suspicious wire transfers.
	6.24	Enhanced checks should be conducted before establishing a business relationship or processing a transaction, where possible, if there are circumstances giving rise to suspicion.
	6.25	In order to demonstrate compliance with the provisions of paragraphs 6.22 to 6.24 above, the screening and any results should be documented, or recorded electronically.
	6.26	If an FI suspects that a transaction is terrorist-related, it should make a report to the JFIU. Even if there is no evidence of a direct terrorist connection, the transaction should still be reported to the JFIU if it looks suspicious for other reasons, as it may emerge subsequently that there is a terrorist link.

Chapter 7 – SUSPICIOUS TRANSACTION REPORTS		
General issues		
s.25A(1), DTROP & OSCO, s.12(1), UNATMO	7.1	Sections 25A of the DTROP and the OSCO make it an offence to fail to disclose where a person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence respectively. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property. Under the DTROP and the OSCO, failure to report knowledge or suspicion carries a maximum penalty of three months' imprisonment and a fine of $50,000.
s.25A(2), DTROP & OSCO, s.12(2), UNATMO	7.2	Filing a report to the JFIU provides FIs with a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided: (a) the report is made before the FI undertakes the disclosed acts and the acts (transaction(s)) are undertaken with the consent of the JFIU; or (b) the report is made after the FI has performed the disclosed acts (transaction(s)) and the report is made on the FI's own initiative and as soon as it is reasonable for the FI to do so.
s.25A(4), DTROP & OSCO, s.12(4), UNATMO	7.3	Once an employee has reported his suspicion to the appropriate person in accordance with the procedure established by his employer for the making of such disclosures, he has fully satisfied the statutory obligation.
s.25A(5), DTROP & OSCO, s.12(5), UNATMO	7.4	It is an offence ("tipping off") to reveal to any person any information which might prejudice an investigation; if a client is told that a report has been made, this would prejudice the investigation and an offence would be committed.
	7.5	Once knowledge or suspicion has been formed the following general principles should be applied: (a) in the event of suspicion of ML/TF, a disclosure should be made even where no transaction has been conducted by or through the FI[46]; (b) disclosures must be made as soon as is reasonably practical after the

[46] 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.

		suspicion was first identified; and (c) FIs must ensure that they put in place internal controls and systems to prevent any directors, officers and employees committing the offence of tipping off the customer or any other person who is the subject of the disclosure. FIs should also take care that their line of enquiry with customers is such that tipping off cannot be construed to have taken place.
	7.6	CDD and ongoing monitoring provide the basis for recognising unusual and suspicious transactions and events. An effective way of recognising suspicious activity is knowing enough about customers, their circumstances and their normal expected activities to recognise when a transaction or instruction, or a series of transactions or instructions, is unusual.
	7.7	FIs must ensure sufficient guidance is given to staff[47] to enable them to form suspicion or to recognise when ML/TF is taking place, taking account of the nature of the transactions and instructions that staff is likely to encounter, the type of product or service and the means of delivery, i.e. whether face to face or remote. This will also enable staff to identify and assess the information that is relevant for judging whether a transaction or instruction is suspicious in the circumstances.
Knowledge vs. suspicion		
	7.8	FIs have an obligation to report where there is knowledge or suspicion of ML/TF. 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.
	7.9	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence.
	7.10	As the types of transactions which may be used for criminal activity are almost unlimited, it is difficult to determine what will constitute a suspicious transaction.

[47] In the context of Chapter 7, staff include appointed insurance agents.

	7.11	The key is knowing enough about the customer's business to recognise that a transaction, or a series of transactions, is unusual and, from an examination of the unusual, whether there is a suspicion of ML/TF. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction should be considered as unusual and the FI should be put on alert.
JFIU "SAFE" Approach	7.12	Where the FI conducts enquiries and obtains what it considers to be a satisfactory explanation of the activity or transaction, it may conclude that there are no grounds for suspicion, and therefore take no further action. However, where the FI's enquiries do not provide a satisfactory explanation of the activity or transaction, it may conclude that there are grounds for suspicion, and must make a disclosure (*see: <www.jfiu.gov.hk/en/str_ask.html>)*.
	7.13	For a person to have knowledge or suspicion, he does not need to know the nature of the criminal activity underlying the money laundering, or that the funds themselves definitely arose from the criminal offence.
	7.14	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 high risk jurisdictions[48] 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. FIs should also be aware of elements of individual transactions that could indicate property involved in terrorist financing. The FATF has issued guidance for FIs in detecting terrorist financing[49]. FIs should be familiar with the characteristics in that guidance, which are grouped under the headings of (i) accounts; (ii) deposits and withdrawals; (iii) wire transfers; (iv) characteristics of the customer or his/her identity; and (v) transactions linked to locations of concern.
	7.15	The OSCO, DTROP and UNATMO prohibit disclosure by the FI or its staff that a suspicious transaction report (STR) has been made which is likely to prejudice any investigation that might be conducted following that disclosure. A risk exists that customers could be unintentionally tipped off when the FI is seeking to perform its CDD obligations during the establishment or course of the business relationship, or when conducting occasional transactions. The customer's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/TF operation. Therefore, if FIs form a suspicion that transactions relate to ML/TF, they should take into account the risk of tipping off when performing the CDD process. FIs should ensure that their employees are aware of and sensitive to these issues when conducting CDD.
Timing and manner of reports		

[48] Guidance on determining high risk jurisdictions is provided at paragraphs 4.15.

[49] Available on the FATF website at www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf

	7.16	When an FI knows or suspects that property represents the proceeds of crime or terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so[50]. The use of a standard form or the use of the e-channel "STREAMS" [51] by registered users is strongly encouraged. Further details of reporting methods and advice may be found at www.jfiu.gov.hk. In the event that an urgent disclosure is required, particularly when the account is part of an ongoing investigation, it should be indicated in the disclosure. Where exceptional circumstances exist in relation to an urgent disclosure, an initial notification by telephone may be considered.
	7.17	Dependent on when knowledge or suspicion arises, disclosures 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.
s.25A(1), DTROP & OSCO, s.12(1), UNATMO	7.18	The law requires the disclosure to be made together with any matter on which the knowledge or suspicion is based. The need for prompt disclosures is especially important where a customer has instructed the FI to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, consideration may be given to contact the JFIU urgently.
Internal reporting		
	7.19	An FI should appoint a Money Laundering Reporting Officer (MLRO) as a central reference point for reporting suspicious transactions. The FI should have measures in place to check, on an ongoing basis that it has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance. The type and extent of the measures to be taken in this respect should be appropriate having regard to the risk of ML/TF and the size of the business.
	7.20	The FI should ensure that the MLRO is of sufficient status within the organisation, and has adequate resources, to enable him to perform his functions.
s.25A(4), DTROP &	7.21	It is the responsibility of the MLRO to consider all internal disclosures he receives in the light of full access to all relevant documentation and

[50] The purpose of disclosure is to fulfil the legal obligations set out in paragraph 7.1. Where FIs want to make a crime report, a report should be made directly to the Hong Kong Police.

[51] STREAMS (Suspicion Transaction Report and Management System) is a web-based platform to assist in the receipt, analysis and dissemination of STRs. Use of STREAMS is recommended, especially for FIs who make frequent reports. Further details may be obtained from the JFIU.

OSCO, s12(4), UNATMO		other parties. However, the MLRO should not simply be that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the MLRO should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfil these functions all FIs must ensure that the MLRO receives full co-operation from all staff and full access to all relevant documentation so that he is in a position to decide whether attempted or actual ML/TF is suspected or known.
	7.22	Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity or suspicious attempted transaction or activity not being disclosed to the JFIU in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary.
	7.23	FIs should establish and maintain 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 disclosure report; and (b) all disclosure reports must reach the MLRO without undue delay.
	7.24	While FIs may wish to set up internal systems that allow staff to consult with supervisors or managers before sending a report to the MLRO, under no circumstances should reports raised by staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The legal obligation is to report as soon as it is reasonable to do so, so reporting lines should be as short as possible with the minimum number of people between the staff with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.
	7.25	All suspicious activity reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.
s.25A(5), DTROP & OSCO, s.12(5),	7.26	The MLRO must acknowledge receipt of the report and at the same time provide a reminder of the obligation regarding tipping off. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.

UNATMO		
	7.27	The reporting of a suspicion in respect of a transaction or event does not remove the need to report further suspicious transactions or events in respect of the same customer. Further suspicious transactions or events, whether of the same nature or different to the previous suspicion, must continue to be reported to the MLRO who should make further reports to the JFIU if appropriate.
	7.28	When evaluating an internal disclosure, the MLRO must take reasonable steps to consider all relevant information, including CDD and ongoing monitoring information available within or to the FI concerning the entities to which the report relates. This may include: (a) making a review of other transaction patterns and volumes through connected accounts; (b) any previous patterns of instructions, the length of the business relationship and reference to CDD and ongoing monitoring information and documentation; and (c) appropriate questioning of the customer per the systematic approach to identifying suspicious transactions recommended by the JFIU[52].
	7.29	As part of the review, other connected accounts or relationships may need to be examined. The need to search for information concerning connected accounts or relationships should strike an appropriate balance between the statutory requirement to make a timely disclosure to the JFIU and any delays that might arise in searching for more relevant information concerning connected accounts or relationships. The evaluation process should be documented, together with any conclusions drawn.
	7.30	If after completing the evaluation, the MLRO decides that there are grounds for knowledge or suspicion, he should disclose the information to the JFIU as soon as it is reasonable to do so after his evaluation is complete together with the information on which that knowledge or suspicion is based. Providing they act 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 a MLRO concludes that there is no suspicion after taking into account all available information. It is however vital for MLROs to keep proper records of their deliberations and actions taken to demonstrate they have acted in reasonable manner.

[52] For details, please see www.jfiu.gov.hk.

Recording internal reports		
	7.31	FIs must establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the staff members subsequently handling the report, the results of the assessment, whether the report resulted in a disclosure to the JFIU, and information to allow the papers relevant to the report to be located.
Records of reports to the JFIU		
	7.32	FIs must establish and maintain a record of all disclosures made to the JFIU. The record must include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located. This register may be combined with the register of internal reports, if considered appropriate.
Post reporting matters		
	7.33	FIs should note that: (a) filing a report to the JFIU only provides a statutory defence to ML/TF in relation to the acts disclosed in that particular report. It does not absolve an FI from the legal, reputational or regulatory risks associated with the account's continued operation; (b) a "consent" response from the JFIU to a pre-transaction report should not be construed as a "clean bill of health" for the continued operation of the account or an indication that the account does not pose a risk to the FI; (c) FIs should conduct an appropriate review of a business relationship upon the filing of a report to the JFIU, irrespective of any subsequent feedback provided by the JFIU; (d) once an FI has concerns over the operation of a customer's account or a particular business relationship, it should take appropriate action to mitigate the risks. 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; (e) relationships reported to the JFIU should be subject to an appropriate review by the MLRO and if necessary the issue should be escalated to the FI's senior management to determine how to handle the relationship to mitigate any potential legal or reputational risks posed by the relationship in line with the FI's business objectives, and its capacity to mitigate the risks identified; and (f) FIs are not obliged to continue business relationships with customers if such action would place them at risk. It is recommended that FIs indicate any intention to terminate a

		relationship in the initial disclosure to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.
s.25A(1)(c) & (2)(a), DTROP & OSCO, s.1 & 12(2)(a), UNATMO	7.34	The JFIU will acknowledge receipt of a disclosure made by an institution under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO. An example of such a letter is given at Appendix B to this guideline. For disclosures submitted via e-channel "STREAM", e-receipt will be issued via the same channel. The JFIU may, on occasion, seek additional information or clarification with an FI of any matter on which the knowledge or suspicion is based.
	7.35	Whilst there are no statutory requirements to provide feedback arising from investigations, the Hong Kong Police and Customs and Excise Department recognise the importance of having effective feedback procedures in place. The JFIU provides feedback both in its quarterly report[53] and upon request, to a disclosing FI in relation to the current status of an investigation.
	7.36	After initial analysis by the JFIU, reports that are to be developed are allocated to financial investigation officers for further investigation. FIs must ensure that they respond to all production orders within the required time limit and provide all of the information or material that falls within the scope of such orders. Where an FI encounters difficulty in complying with the timeframes stipulated, the MLRO 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	7.37	During a law-enforcement investigation, an FI may be served with a Restraint Order, designed to freeze particular funds or property pending the outcome of an investigation. An FI must ensure that it is able to freeze the relevant property that is the subject of the order. It should be noted that the Restraint Order may not apply to all funds or property involved within a particular business relationship and FIs should consider what, if any, funds or property may be utilised subject to having obtained the appropriate consent from the JFIU.

[53] 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 through the JFIU's website at www.jfiu.gov.hk. A password is required, details may be found under the typologies and feedback section of the website or by contacting the JFIU directly.

s.3, DTROP, s.8, OSCO, s13, UNATMO	7.38	Upon the conviction of a defendant, a court may order the confiscation of his criminal proceeds and an FI may be served with a Confiscation Order in the event that it holds funds or other property belonging to that defendant that are deemed by the Courts to represent his benefit from the crime. A court may also order the forfeiture of property where it is satisfied that the property is terrorist property.

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 which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time 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 which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time 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 permanent 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.*

Important Note		
		The International Association of Insurance Supervisors (IAIS) has published relevant examples and indicators involving insurance in a document called "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded from IAIS website at ***http://www.iaisweb.org****. The list will be updated periodically to include additional examples identified. IIs are advised to regularly browse the website for latest information.*

Annex II - Examples of money laundering schemes[54]		
Life Insurance		
		Case 1 *In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over US$1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute. This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.* ***Case 2*** *A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two 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.*

[54] *Majority of the examples of money laundering schemes in this annex are extracted from the IAIS document "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded at* ***http://www.iaisweb.org/.***

		Case 3 *Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.* *Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean.* *To date, this investigation has identified that over US$29 million was laundered through this scheme, of which over US$9 million has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.* ***Case 4*** *An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.* ***Case 5*** *On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank accounts and then transferred to an account in another jurisdiction. The drug trafficker then entered into a US$75,000 life*

		insurance policy. Payment for the policy was made by two separate wire transfers from the overseas accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy. ***Case 6*** *A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around US$400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.* ***Case 7*** *A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of US$1 million in case of death. The other was a mixed insurance with value of over half this amount.* ***Case 8*** *A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life-insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around US$7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.*
Reinsurance		
		Case 1 *An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer 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.
Intermediaries		
		Case 1 *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 raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, 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 the raising suspicions with the insurance company.* ***Case 2*** *Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client 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 the 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 client stating that there was now a change in circumstances, and they would have to close the policy suffering the 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 closed 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 3*** *An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary.* *In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.* ***Case 4*** *A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around US$400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.*
Other examples		

		Single premiums *An example involves the purchase of large, single premium insurance policies and their subsequent rapid redemption. A money launderer does this to obtain payment from an insurance company. The person may face a redemption fee or cost, but this is willingly paid in exchange for the value that having funds with an insurance company as the immediate source provider.* *In addition, the request for early encashment of single premium policies, for cash or settlement to an individual third party may arouse suspicion.* ***Return premiums*** *There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:* *(a) a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;* *(b) return premium being credited to an account different from the original account;* *(c) requests for return premiums in currencies different from the original premium; and* *(d) regular purchase and cancellation of policies.* ***Overpayment of premiums*** *Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be*

		unwilling to confront a customer who is both profitable to the company and important to his own success. *The overpayment of premiums, has been used as a method of money laundering. Insurers should be especially vigilant where:* • *the overpayment is over a certain size (say US$10,000 or equivalent);* • *the request to refund the excess premium was to a third party;* • *the assured is in a jurisdiction associated with money laundering; and* • *where the size or regularity of overpayments is suspicious.* ***High brokerage / third party payments / strange premium routes*** *High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.* ***Assignment of claims*** *In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.*
Important Note		
		Apart from the above examples of money laundering schemes, the FATF has also published annually detailed typologies involving insurance supported by useful case examples in documents called "Money Laundering & Terrorist Financing Typologies". The documents can be

		downloaded at the publications section of FATF website at ***http://www.fatf-gafi.org****. IIs are advised to regularly browse the website for latest information.*

Chapter 8 – RECORD-KEEPING		
General legal and regulatory requirements		
	8.1	Record-keeping is an essential part of the audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps the investigating authorities to establish a financial profile of a suspect, trace the criminal or terrorist property or funds and assists the Court to examine all relevant past transactions to assess whether the property or funds are the proceeds of or relate to criminal or terrorist offences.
	8.2	FIs should maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements under the AMLO, this guideline and other regulatory requirements, that are appropriate to the scale, nature and complexity of their businesses. This is to ensure that: (a) the audit trail for funds moving through an FI that relate to any customer and, where appropriate, the beneficial owner of the customer, account or transaction is clear and complete; (b) any customer and, where appropriate, the beneficial owner of the customer can be properly identified and verified; (c) all customer and transaction records and information are available on a timely basis to RAs, other authorities and auditors upon appropriate authority; and (d) FIs are able to comply with any relevant requirements specified in other sections of this guideline and other guidelines issued by the RAs, including, among others, records of customer risk assessment (see paragraph 3.8), registers of suspicious transaction reports (see paragraph 7.32) and training records (see paragraph 9.9).
Retention of records relating to customer identity and transactions		
s.20(1)(b)(i), Sch. 2	8.3	FIs 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 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) any additional information in respect of a customer and/or beneficial owner of the customer that may be obtained for the purposes of EDD or ongoing monitoring; (c) where applicable, the original or a copy of the documents, and a

s.2(1)(c), Sch. 2 s.20(1)(b)(ii), Sch. 2		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; risk assessment form) and business correspondence[55] 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).
s.20(3), Sch. 2	8.4	All documents and records mentioned in paragraph 8.3 should be kept throughout the business relationship with the customer and for a period of at least five years after the end of the business relationship.
s.20(1)(a), Sch. 2	8.5	FIs should maintain the original or a copy of the documents, and a record of the data and information, obtained in connection with the transaction, which should be sufficient to permit reconstruction of individual transactions and establish a financial profile of any suspect account or customer. These records may include the following: (a) the identity of the parties to the transaction; (b) the nature and date of the transaction; (c) the type and amount of currency involved; (d) the origin of the funds (if known); (e) the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.; (f) the destination of the funds; (g) the form of instruction and authority; and (h) the type and identifying number of any account involved in the transaction (where applicable).
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.
	8.6a	*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*

[55] FIs are 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.

		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	8.7	If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer.
s.20(4), Sch. 2	8.8	An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or customer for a period specified by the RA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice.
Records kept by intermediaries		
s.18(4)(b), Sch. 2	8.9	Where customer identification and verification documents are held by an intermediary on which the FI is relying to carry out CDD measures, the FI concerned remains responsible for compliance with all record-keeping requirements. FIs should ensure that the intermediaries being relied on have 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 8.8), and that documents and records will be provided by the intermediaries as soon as reasonably practicable after the intermediaries receive the request from the FIs.
s.18(4)(a), Sch. 2	8.10	For the avoidance of doubt, FIs that rely on intermediaries for carrying out a CDD measure should immediately obtain the information that the intermediary has obtained in the course of carrying out that measure, for example, name and address.
	8.11	An FI should ensure that an intermediary will pass the documents and records to the FI, upon termination of the services provided by the intermediary.

Part 3, Sch. 2	8.12	Irrespective of where identification and transaction records are held, FIs are required to comply with all legal and regulatory requirements in Hong Kong, especially Part 3 of Schedule 2.
Record-keeping obligations by individual insurance agents		
	8.13a	*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 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 a RA.* *This guidance applies to individual insurance agents only and does not apply to insurance agencies.*

Chapter 9 – STAFF TRAINING		
	9.1	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	Staff[56] should be trained in what they need to do to carry out their particular roles in the FI with respect to AML/CFT. This is particularly important before new staff commence work.
	9.3	FIs should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training.
	9.4	The timing and content of training packages for different groups of staff will need to be adapted by individual FIs for their own needs, with due consideration given to the size and complexity of their business and the type and level of ML/TF risk.
	9.5	FIs should provide appropriate AML/CFT training to their staff. The frequency of training should be sufficient to maintain the AML/CFT knowledge and competence of the staff.
	9.6	Staff should be made aware of: (a) their FI's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO; (b) any other statutory and regulatory obligations that concern their FIs and themselves under the DTROP, the OSCO, the UNATMO, the UNSO and the AMLO, and the possible consequences of breaches of these obligations; (c) the FI's policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting; and (d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in the FI with respect to AML/CFT.
	9.7	In addition, the following areas of training may be appropriate for certain groups of staff:

[56] In the context of Chapter 9, staff include appointed insurance agents.

		(a) all new staff, irrespective of seniority: (i) an introduction to the background to ML/TF and the importance placed on ML/TF by the FI; and (ii) the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of "tipping-off"; (b) members of staff who are dealing directly with the public (e.g. front-line personnel, appointed insurance agents who act on behalf of authorized insurers): (i) the importance of their role in the FI's ML/TF strategy, as the first point of contact with potential money launderers; (ii) the FI's policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities; and (iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required; (c) back-office staff, depending on their roles: (i) appropriate training on customer verification and relevant processing procedures; and (ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions; (d) managerial staff including internal audit officers and COs: (i) higher level training covering all aspects of the FI's AML/CFT regime; and (ii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU; and (e) MLROs: (i) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and (ii) training to keep abreast of AML/CFT requirements/developments generally.
	9.8	FIs are 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. FIs may consider including available FATF papers and typologies as part of the training materials. All materials should be up-to-date and in line with current requirements and standards.

	9.9	No matter which training approach is adopted, FIs should monitor and 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[57].
	9.10	FIs should monitor the effectiveness of the training. This may be achieved by: (a) testing staff's understanding of the FI's policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions; and (b) monitoring the compliance of staff with the FI's AML/CFT systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken.

[57] For insurance institutions, the records should be kept for a minimum of 3 years from the assessment date, i.e. 31 July of each year.

Chapter 10 – WIRE TRANSFERS		
General requirements		
	10.1	This Chapter primarily applies to authorized institutions and money service operators. Other FIs should also comply with section 12 of Schedule 2 and the guidance provided in this Chapter if they act as an ordering institution, an intermediary institution or a beneficiary institution as defined under the AMLO. Where an FI is the originator or recipient of a wire transfer, it is not acting as an ordering institution, an intermediary institution or a beneficiary institution and thus is not required to comply with the requirements under section 12 of Schedule 2 or this Chapter in respect of that transaction.
s.1(4) & s.12(11), Sch. 2	10.2	A wire transfer is a transaction carried out by an institution (the ordering institution) on behalf of a person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution), which may be the ordering institution or another institution, whether or not one or more other institutions (intermediary institutions) participate in completion of the transfer of the money. An FI should follow the relevant requirements set out in this Chapter with regard to its role in a wire transfer.
	10.3	The requirements set out in section 12 of Schedule 2 and this Chapter are also applicable to wire transfers using cover payment mechanism (e.g. MT202COV payments)[58].
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 if each of them acts on its own behalf; (b) a wire transfer between an FI and a foreign institution[59] if each of them acts on its own behalf; (c) a wire transfer if: (i) it arises from a transaction that is carried out using a credit card or debit card (such as withdrawing money from a bank account through an automated teller machine with a debit card, obtaining

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

[59] 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 a financial institution.

		a cash advance on a credit card, or paying for goods or services with a credit or debit card), except when the card is used to effect a transfer of money; and (ii) the credit card or debit card number is included in the message or payment form accompanying the transfer.
Ordering institutions		
s.12(3) & (5), Sch. 2	10.5	An ordering institution must ensure that a wire transfer of amount equal to or above HK$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, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth; (d) the recipient's name; and (e) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
s.12(3) , (3A) & (5), Sch. 2	10.6	An ordering institution must ensure that a wire transfer of amount below HK$8,000 (or an equivalent amount in any other currency) is accompanied by the following originator and recipient information : (a) the originator's name; (b) the number of the originator's account maintained with the ordering institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned by the ordering institution; (c) the recipient's name; and (d) the number of the recipient's account maintained with the beneficiary institution and to which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the beneficiary institution.
	10.7	The unique reference number assigned by the ordering institution or beneficiary institution referred to in paragraphs 10.5 and 10.6 should permit traceability of the wire transfer.

	10.8	For a wire transfer of amount equal to or above HK$8,000 (or an equivalent amount in any other currency), an ordering institution must ensure that the required originator information accompanying the wire transfer is accurate.
s.3(1)(c) & (d) , Sch. 2	10.9	For an occasional wire transfer involving an amount equal to or above HK$8,000 (or an equivalent amount in any other currency), an ordering institution must verify the identity of the originator. For an occasional wire transfer below HK$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 HK$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[60], an ordering institution may choose not to include the complete required originator information in the wire transfer but only include the originator's account number or, in the absence of an account, a unique reference number, provided that the number permits traceability of the wire transfer.
s.12(6), Sch. 2	10.12	If an ordering institution chooses not to include complete required originator information as stated in paragraph 10.11, it must, on the request of the institution to which it passes on the transfer 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 authorities immediately upon request.
Intermediary institutions		

[60] 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 financial institutions located in Hong Kong.

s.12(8), Sch. 2	10.13	An intermediary institution must ensure that all originator and recipient information which accompanies the wire transfer is retained with the transfer and is transmitted to the institution to which it passes on the transfer instruction.
	10.14	Where technical limitations prevent the required originator or recipient information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary institution should keep a record, for at least five years, of all the information received from the ordering institution or another intermediary institution. The above requirement also applies to a situation where technical limitations prevent the required originator or recipient information accompanying a domestic wire transfer from remaining with a related cross-border wire transfer.
s.19(2), Sch. 2	10.15	An intermediary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that have not been complied with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
s.12(10)(a), Sch.2	10.16	In respect of the risk-based policies and procedures referred to in paragraph 10.15, if a cross-border wire transfer is not accompanied by the required originator information or required recipient information, the intermediary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the intermediary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
s.12(10)(b), Sch.2	10.17	If the intermediary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.

Beneficiary institutions		
s.19(2), Sch. 2	10.18	A beneficiary institution must establish and maintain effective procedures for identifying and handling incoming wire transfers that do not comply with the relevant originator or recipient information requirements, which include: (a) taking reasonable measures (e.g. post-event monitoring) to identify domestic or cross-border wire transfers that lack required originator information or required recipient information; and (b) having risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator information or required recipient information; and (ii) the appropriate follow-up action.
s.12(9)(a) & s.12(10)(a), Sch.2	10.19	In respect of the risk-based policies and procedures referred to in paragraph 10.18, if a domestic or cross-border wire transfer is not accompanied by the required originator information or required recipient information, the beneficiary institution must as soon as reasonably practicable, obtain the missing information from the institution from which it receives the transfer instruction. If the missing information cannot be obtained, the beneficiary institution should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the risk of ML/TF involved.
s.12(9)(b) & s.12(10)(b), Sch.2	10.20	If the beneficiary institution is aware that the accompanying information that purports to be the required originator information or required recipient information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.
s.3(1)(c), Sch. 2	10.21	For a wire transfer of amount equal to or above HK$8,000 (or an equivalent amount in any other currency), a beneficiary institution should verify the identity of the recipient, if the identity has not been previously verified.

APPENDIX A

Examples of reliable and independent sources for customer identification purposes

s.2(1)(a)(iv) & s.2(1)(d)(i)(D), Sch. 2	1	The identity of an individual physically present in Hong Kong should be verified by reference to their Hong Kong identify card or travel document. FIs should always identify and/or verify a Hong Kong resident's identity by reference to their Hong Kong identity card, certificate of identity or document of identity. The identity of a non-resident should be verified by reference to their valid travel document.
	2	For non-resident individuals who are not physically present in Hong Kong, FIs may identify and or verify their identity by reference to the following documents: (a) a valid international passport or other travel document; or (b) a current national (i.e. Government or State-issued) identity card bearing the photograph of the individual; or (c) current valid national (i.e. Government or State-issued) driving license[61] incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority.
	3	Travel document means a passport or some other document furnished with a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder. The following documents constitute travel documents for the purpose of identity verification: (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 Organisation Convention/Seafarers Identity Document 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.

[61] For avoidance of doubt, international drivers permits and licences are not acceptable for this purpose.

	4	For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card[62], their identity should be verified by reference to the minor's Hong Kong birth certificate. Whenever establishing relations with a minor, the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified in accordance with the above requirements.
	5	An FI may identify and/or verify a corporate customer by performing a company registry search in the place of incorporation and obtaining a full company search report, which confirms the current reference to a full company particulars search (or overseas equivalent).
	6	For jurisdictions that do not have national ID cards and where customers do not have a travel document or driving licence with a photograph, FIs may, exceptionally and applying a risk-based approach, accept other documents as evidence of identity. Wherever possible such documents should have a photograph of the individual.

[62] All residents of Hong Kong who are aged 11 and above are required to register for an identity card. Hong Kong permanent residents will have a Hong Kong Permanent Identity Card. The identity card of a permanent resident (i.e. a Hong Kong Permanent Identity Card) will have on the front of the card a capital letter "A" underneath the individual's date of birth.

APPENDIX B

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

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

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

Date: 2012-XX-XX

Money Laundering Reporting Officer,
XXXXXXX.

Fax No. : XXXX XXXX

Dear Sir/Madam,

Suspicious Transaction Report ("STR")

JFIU No.	Your Reference	Date Received
XX	XX	XX

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

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

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

Yours faithfully,

(XXXXX)
for Head, Joint Financial Intelligence Unit

PERSONAL DATA

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

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

Our Ref. :
Your Ref :

2012-XX-XX

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

Dear Sir/Madam,

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

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

JFIU No.	Your Reference	Dated
XX	XX	XX

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

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

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

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

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

Yours faithfully,

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

c.c. OC Case

Annex A

S/N	Account holder	Account Number
1.		

GLOSSARY OF KEY TERMS AND ABBREVIATIONS

Terms / abbreviations	Meaning
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
AML/CFT	Anti-money laundering and counter financing of terrorism
BO	Banking Ordinance (Cap. 155)
CDD	Customer due diligence
CO	Compliance officer
Connected parties	Connected parties to a customer include the beneficial owner and any natural person having the power to direct the activities of the customer. For the avoidance of doubt the term connected party will include any director, shareholder, beneficial owner, signatory, trustee, settlor/grantor/founder, protector(s), or defined beneficiary of a legal arrangement.
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FI(s)	Financial institution(s)
IAIS	*International Association of Insurance Supervisors*
IO	Insurance Ordinance (Cap. 41)
II(s)	*Insurance institution(s), referring to authorized insurers, reinsurers, appointed insurance agents and authorized insurance brokers carrying on or advising on long term business.*
Individual	Individual means a natural person, other than a deceased natural person.
JFIU	Joint Financial Intelligence Unit

Minor	Minor means a person who has not attained the age of 18 years [Interpretation and General Clauses Ordinance (Cap. 1) - section 3].
MLRO	Money laundering reporting officer
ML/TF	Money laundering and/or terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
PEP(s)	Politically exposed person(s)
RA(s)	Relevant authority (authorities)
RBA	Risk-based approach to CDD and ongoing monitoring
Schedule 2	Schedule 2 to the AMLO
SDD	Simplified customer 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).
SFO	Securities and Futures Ordinance (Cap. 571)
STR(s)	Suspicious transaction report(s); also referred to as reports or disclosures
Trust	For the purposes of the 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 form) is in place.
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)