



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

Consultation Paper on (1) the Proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing and (2) the Proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities and Futures Commission for Associated Entities

September 2011



Table of Contents

Foreword	1
Personal Information Collection Statement	2
Consultation on (1) the Proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing and (2) the Proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities and Futures Commission for Associated Entities	4
Introduction	4
Background	4
Overview of the Guideline	5
Key differences between the AMLGN and the proposed Guideline	7
Seeking comments	9
Appendix 1 - Proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing	
Appendix 2 - Proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities Futures Commission for Associated Entities	

.



Foreword

The Securities and Futures Commission (SFC) invites the public to submit written comments on this Consultation Paper on (1) the Proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing and (2) the Proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities and Futures Commission for Associated Entities, **no later than 18 November 2011**.

Any person wishing to submit comments on behalf of any organization should provide details of the organization whose views they represent. In addition, respondents who wish to suggest alternative approaches are encouraged to submit the proposed text of possible amendments that would be necessary to incorporate their suggestions into the two proposed guidelines.

Please note that the names of commentators and the contents of their submissions may be published by the SFC on its website and in other documents to be published by the SFC. In this connection, please read the Personal Information Collection Statement attached to this consultation paper.

You may not wish your name and / or submission to be published by the SFC. If this is the case, please state that you wish your name and / or submission to be withheld from publication when you make your submission.

Written comments may be sent

By mail to: Intermediaries Supervision Department
Securities and Futures Commission
8th Floor, Chater House
8 Connaught Road Central
Hong Kong

By fax to: (852) 2284 4660

By on-line submission: <http://www.sfc.hk>

By e-mail to: aml_guideline@sfc.hk

All submissions received before expiry of the consultation period will be taken into account before the proposals are finalized and a consultation conclusions paper will be published in due course.



Personal Information Collection Statement

1. This Personal Information Collection Statement (PICS) is made in accordance with the guidelines issued by the Privacy Commissioner for Personal Data. The PICS sets out the purposes for which your Personal Data¹ will be used following collection, what you are agreeing to with respect to the SFC's use of your Personal Data and your rights under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO).

Purpose of Collection

2. The Personal Data provided in your submission to the SFC in response to this consultation paper may be used by the SFC for one or more of the following purposes:
 - (a) to administer the relevant provisions² and codes and guidelines published pursuant to the powers vested in the SFC;
 - (b) in performing the SFC's statutory functions under the relevant provisions;
 - (c) for research and statistical purposes;
 - (d) for other purposes permitted by law.

Transfer of Personal Data

3. Personal Data may be disclosed by the SFC to members of the public in Hong Kong and elsewhere, as part of the public consultation on this consultation paper. The names of persons who submit comments on this consultation paper together with the whole or part of their submission may be disclosed to members of the public. This will be done by publishing this information on the SFC's website and in documents to be published by the SFC during the consultation period or at its conclusion.

Access to Data

4. You have the right to request access to and correction of your Personal Data in accordance with the provisions of the PDPO. Your right of access includes the right to obtain a copy of your Personal Data provided in your submission on this consultation paper. The SFC has the right to charge a reasonable fee for processing any data access request.

Retention

5. Personal Data provided to the SFC in response to this consultation paper will be retained for such period as may be necessary for the proper discharge of the SFC's functions.

¹ Personal Data means "personal data" as defined in the Personal Data (Privacy) Ordinance (Cap. 486).

² As defined in Section 1, Part 1, Schedule 1 to the Securities and Futures Ordinance (Cap. 571) (**SFO**).



Enquiries

6. Any enquiries regarding the Personal Data provided in your submission on this consultation paper, or requests for access to Personal Data or correction of Personal Data, should be addressed in writing to:

The Data Privacy Officer
Securities and Futures Commission
8th Floor, Chater House
8 Connaught Road Central
Hong Kong

A copy of the Privacy Policy Statement adopted by the SFC is available upon request.



Consultation on (1) the Proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing and (2) the Proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities and Futures Commission for Associated Entities

Introduction

1. Under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO), a relevant authority³ (RA) may publish in the Gazette any guideline that it considers appropriate for providing guidance in relation to the provisions of Schedule 2 of the AMLO, including customer due diligence (CDD) and record keeping requirements.
2. The SFC has prepared a proposed Guideline on Anti-Money Laundering and Counter-Terrorist Financing (the Guideline) to provide guidance to assist licensed corporations (LCs) and their officers and staff to comply with the AMLO and other applicable anti-money laundering (AML) / counter-terrorist financing (CFT) legislation and regulatory requirements. In particular, the key objective of the Guideline is to help LCs implement AML/CFT policies, procedures and controls in the relevant operational areas so as to meet the relevant statutory and regulatory requirements.
3. The SFC would like to invite comments from the public on the proposed Guideline, which is set out in Appendix 1 to this consultation paper.
4. Separately, associated entities⁴ (AEs) are also required, under the proposed Prevention of Money Laundering and Terrorist Financing Guideline Issued by the Securities and Futures Commission for Associated Entities (Guideline for AEs), to implement AML/CFT policies, procedures and controls similar to those in the Guideline. The SFC therefore would also like to invite comments from the public on the proposed Guideline for AEs, which is set out in Appendix 2 to this consultation paper.

Background

5. The enacted AMLO was gazetted on 8 July 2011 after two rounds of consultation conducted by the Financial Services and Treasury Bureau (FSTB); and it shall come into effect on 1 April 2012. The purpose of the AMLO is to enhance the AML/CFT regime in Hong Kong in respect of the financial sectors so as to meet requirements set by the Financial Action Task Force (FATF), especially in respect of CDD and record keeping.
6. As the AMLO provides for a uniform set of requirements applicable to all financial institutions in the banking, securities, insurance and remittance and money changing sectors (FIs), the four RAs, in consultation with the FSTB, have together drafted a set of guidelines containing generic guidance that is applicable to all FIs.

³ The Hong Kong Monetary Authority, SFC, Insurance Authority and the Customs and Excise Department have been designated as the relevant authorities for supervising the AML/CFT compliance by their respective sectors.

⁴ As defined in Section 1, Part 1, Schedule 1 to the SFO.



7. Furthermore, individual RAs may add supplementary or sector-specific guidance that is necessary or appropriate for their respective sectors. Such supplementary or sector-specific guidance is put in italics for ease of identification in the proposed Guideline. The SFC is of the view that the generic guidance applicable to all FIs is generally adequate and appropriate to the securities sector, and further guidance will only be needed for giving examples of sector-specific suspicious transaction indicators and making some minor clarifications.
8. 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, it is accepted that there exists no single set of universally applicable implementation measures. As such, senior management of FIs may tailor-make these measures to their particular business risk profile⁵. Where there are to be departures from the guidance provided, FIs should document the rationale for so doing and stand prepared to justify departures to the RAs.
9. Soft consultation has also been conducted by the RAs to gauge feedback from their respective sectors. In particular, selected representatives from the broking, fund management and financial planning industry have been consulted by the SFC before completing the proposed Guideline.
10. The Guideline will be published under the AMLO and the Securities and Futures Ordinance (SFO). When this is primarily intended for use by LCs, their officers and staff, registered institutions should also have regard to the examples of securities sector-specific suspicious transaction indicators in the Guideline, in addition to the similar guideline issued by the Hong Kong Monetary Authority.
11. This Guideline will replace the existing Prevention of Money Laundering and Terrorist Financing Guidance Note (AMLGN) published by the SFC which currently applies to LCs as well as AEs. Given that the AMLO does not apply to AEs, to avoid possible confusion, a separate guideline will be published under the SFO to cover AEs.

Overview of the Guideline

12. The Guideline is divided into 10 chapters and two appendices:
 - (a) Chapter 1 sets out how the Guideline is to be used and interpreted and the persons⁶ to which the Guideline applies. It also provides an overview of the AML/CFT regime in Hong Kong.
 - (b) Chapter 2 provides practical guidance as to how an FI should implement appropriate AML/CFT policies, procedures and controls including group policies for business conducted outside Hong Kong.
 - (c) Guidance is offered in Chapter 3 on how an FI should use a risk-based approach to determine the extent of CDD measures and ongoing monitoring to

⁵ There are however some mandatory requirements (e.g. the company registry search) with which all FIs must comply.

⁶ For ease of identification, when the Guideline only applies to LCs and not FIs in general, references to FIs are retained in the generic guidance to show that it is common to all FIs. In the supplementary or sector-specific guidance applicable only to the securities sector, references to LCs are made.



be adopted for its individual customers so that resources can be allocated in the most efficient way.

- (d) Chapter 4 provides extensive guidance on the CDD requirements for FIs under the AMLO and how they can be met. It lists out the steps an FI should take when carrying out CDD and cites examples of relevant information that should be obtained. Detailed guidance is further given in relation to
 - (i) CDD to be conducted according to different types of customers e.g., natural persons, corporations and partnerships;
 - (ii) the types of customers to which simplified customer due diligence (SDD) or enhanced (customer) due diligence (EDD) or special requirements can or should be applied under the AMLO;
 - (iii) CDD to be conducted on beneficial owners, persons purporting to act on behalf of customers and pre-existing customers;
 - (iv) timing of identification and verification of identity; and
 - (v) keeping customer information up-to-date.
- (e) Chapter 5 explains what is entailed under the ongoing monitoring requirements of the AMLO for FIs, and highlights the important role proper ongoing monitoring plays in the detection of suspicious activities which may indicate money laundering (ML) and/or terrorist financing (TF).
- (f) An overview of financial sanctions and TF is provided in Chapter 6 which also provides guidance on compliance with the relevant sanction regulations and legislation on TF.
- (g) Chapter 7 assists FIs to comply with their obligations to report suspicions of ML/TF. This chapter sets out the role and responsibilities of the money laundering reporting officer (MLRO) of an FI as a central reference point for reporting suspicious transactions. Examples of suspicious transaction indicators including some that are particularly relevant to the securities sector are also provided in this chapter.
- (h) Chapter 8 explains what is entailed under the record-keeping requirements of the AMLO for FIs. It gives examples of the documents that should be retained, and sets out the period and manner in which the records should be kept.
- (i) Guidance on staff training is found in Chapter 9, suggesting, inter alia, elements that should be included in training provided to different groups of staff.
- (j) Chapter 10 provides guidance relating to the wire transfer provisions in the AMLO and compliance guidance where the provisions apply to an FI.
- (k) Appendix A is a supplement to Chapter 4. It lists out additional sources of documents, data or information that are reliable and independent for customer identification purposes which can be used by FIs during the CDD process.



- (l) Examples of correspondence from Joint Financial Intelligence Unit (JFIU) regarding whether an FI may deal with the property of a particular customer / account that is the subject of a suspicious transaction disclosure to the JFIU are found in Appendix B.

Key differences between the AMLGN and the proposed Guideline

- 13. The vast majority of changes and additional requirements introduced in the proposed Guideline are specific requirements under the AMLO or are needed to reflect the latest FATF standards.
- 14. The key differences between the AMLGN and the proposed Guideline that have received much industry feedback during the soft consultation are highlighted below.

Persons purporting to act on behalf of customers

- 15. Under section 2(1)(d) of Schedule 2 to the AMLO, FIs should identify all persons purporting to act on behalf of customers, take reasonable measures to verify their identities and verify their authority to act on behalf of the customers.
- 16. The AMLO was modelled upon the FATF's standard which states that for customers that are legal persons or legal arrangements, FIs should be required to verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person. Concerns were expressed over the broad meaning of "a person purporting to act on behalf of the customer" and suggestions were made to carve out certain types of person, such as traders who could place orders on their company's behalf.
- 17. Other FIs had also raised concerns over the practicality of obtaining a verification of both these persons' authority to act and identification of such persons, especially for customers with a long list of authorized signatories. After much deliberation, it was decided to clarify in the proposed Guideline that as a general rule, FIs should verify the identity of those authorized to give instructions for the movement of funds or assets. Furthermore, some flexibility has been provided in the proposed Guideline as to what measures would be considered reasonable for verifying the identity of a person purporting to act on behalf of a customer. For example, para. 4.9.19 of the proposed Guideline presently provides further methods in verifying the identities of account signatories, which include allowing an FI to adopt a streamlined approach in verifying the identities of account signatories based on its risk assessment of the customer where the customer is an FI or a listed company.

Question 1: *Do you think paras 4.4.1, 4.4.3 and 4.9.19 together provide sufficient guidance to assist FIs to comply with the requirement of taking reasonable measures to verify the identity of persons purporting to act on behalf of customers? If not, please suggest further examples or alternative measures with reasons.*

Wire transfers

- 18. The AMLO imposes special requirements on FIs when carrying out wire transfers, such as the need to verify and record various identification information of the originator of the



wire transfer, and include the information in the message or payment form accompanying the wire transfer.

19. A wire transfer is defined under Part 1 of Schedule 2 to the AMLO as “a transaction carried out by an institution (the ordering institution) on behalf of a person 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 (the intermediary institutions) participate in completion of the transfer of the money”.
20. There had been some discussions during the soft consultation as to whether LCs would ordinarily be considered to carry out wire transfers. The general consensus was that LCs would typically only be the originators or recipients/beneficiaries in wire transfer transactions. The Insurance Authority held the same view with regard to insurance institutions. Following deliberation among the RAs and the FSTB, a chapter giving generic guidance on the wire transfer provisions (Chapter 10) was included in the proposed Guideline. This chapter now clarifies in para. 10.1 that the wire transfer provisions and hence the guidance in Chapter 10 primarily apply to authorized institutions and money service operators and seeks to better explain as to when the wire transfer provisions do not apply to other FIs.

Question 2: *Do you think Chapter 10, particularly para. 10.1, is sufficiently clear as to when the wire transfer provisions do not apply to an LC? If not, what further guidance may be useful in this respect?*

Performance of a company registry search

21. The proposed Guideline requires an FI to perform a company registry search and obtain a full company search report⁷ in respect of all locally incorporated non-listed companies and companies incorporated in jurisdictions which have a public company registry as part of the CDD process. Under the existing AMLGN (para. 6.4.4), such is an additional measure only for higher risk categories of customers or where there is any doubt as to the identity of the beneficial owners, shareholders, directors, etc of the corporate customer.
22. As explained in para. 4.9.12, a company registry can:
 - (a) confirm that 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.
23. Whilst this requirement would increase compliance costs, given that a company registry search can now be conducted on-line in Hong Kong for a low fee, on balance it was felt that FIs should perform this search at the account opening stage.

⁷ Alternatively, the FI may obtain from the customer a certified true copy of a full company search report. Such should be certified by the relevant company registry wherever possible. For the avoidance of doubt, it is not sufficient for the report to be self-certified by the customer.



Question 3: Do you agree that the benefits of performing a company registry search as an independent, effective means of confirming a corporate customer's current status and verifying the names of its directors and shareholders outweigh the costs?

Nominee companies

24. Currently under section 4(3) of Schedule 2 to the AMLO, an FI may apply SDD whereby it is not required to identify and verify the beneficial owners in relation to a customer if the customer is another FI.
25. In the fund distribution business, it is common for the fund distributor (e.g. a bank or an independent financial adviser, which are both FIs) to open an account with a fund house (another FI) in the name of a nominee company for holding fund units on behalf of the customers of the fund distributor. The fund industry was concerned that whether SDD would not be available in such circumstances as the nominee company might appear to be the customer of the fund house rather than the FI fund distributor. However, as fund distributors might not wish to disclose information about their clients for legitimate commercial reasons, fund houses would not be able to identify and verify the beneficial owners of the fund units held by the nominee company.
26. To address the above concern, para. 4.10.6 has been drafted such that, subject to certain safeguards, the fund distributor is regarded as the customer of the fund house and not the nominee company. The safeguards include the requirements that the fund distributor is an FI as defined under the AMLO; has conducted CDD on the underlying customers of the fund; and is authorised to operate the account which is in the name of the nominee company pursuant to a contractual document or agreement.

Question 4: Para. 4.10.6 covers fund distribution activities involving the holding of fund units by nominee companies. Do you think that there are other types of business relationships involving nominee companies controlled by an FI distributor that should also be covered by this provision? If so, please provide details with reasons.

Staff training

27. Staff training is an important element of an effective system to prevent and detect ML/TF activities. Para. 9.10 suggests that an FI should monitor the effectiveness of staff training.

Question 5: Do you agree that FIs should implement a clear and well articulated policy for ensuring that relevant staff receive adequate AML/CFT training and monitor its effectiveness?

Seeking comments

28. The SFC welcomes any comments from the public and the industry on the questions raised in this consultation paper; the proposed Guideline in Appendix 1; and the proposed Guideline for AEs in Appendix 2 to this consultation paper. Please submit comments to the SFC in writing by no later than 18 November 2011.



Appendix 1

PROPOSED GUIDELINE ON ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING

**Effective Date**

This Guideline will become effective on 1 April 2012 and supersedes the Prevention of Money Laundering and Terrorist Financing Guidance Note dated September 2009.



CONTENTS

	Page
Chapter 1 Overview	1
Chapter 2 AML/CFT systems and business conducted outside Hong Kong	7
Chapter 3 Risk-based approach.....	11
Chapter 4 Customer due diligence	14
Chapter 5 Ongoing monitoring	44
Chapter 6 Financial sanctions and terrorist financing	47
Chapter 7 Suspicious transaction reports.....	50
Chapter 8 Record keeping	59
Chapter 9 Staff training	61
Chapter 10 Wire transfers	63
Appendix A Other reliable and independent sources for customer identification purposes	69
Appendix B Sample correspondence issued by the JFIU.....	71
Glossary of key terms and abbreviations	75



Chapter 1 – OVERVIEW

Introduction

	1.1	The Guideline is published under section 7 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (the AMLO).
	1.1a	<i>The Guideline is also published under section 399 of the Securities and Futures Ordinance, Cap. 571 (the SFO).</i>
	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.
	1.2a	<i>Where applicable, interpretation of other words or phrases should follow those set out in the SFO.</i>
	1.3	This Guideline is issued by the SFC for giving guidance to licensed corporations (LCs). In general, the guidance provided in the Guideline in Chapters 1-10 to LCs is not different from the guidance provided by other relevant authorities (RAs) under their respective regulatory regimes. To the extent that the SFC sees fit to provide supplementary guidance in Chapters 1-10, such will be put in italics for ease of identification.
	1.4	<p>The Guideline is intended for use by financial institutions (FIs) and their officers and staff. The purposes of the Guideline are to:</p> <ul style="list-style-type: none"> (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.
	1.4a	<i>In addition to the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the Hong Kong Monetary Authority, registered institutions (RIs) are required to have regard to paragraphs 7.38 and 7.39 of this Guideline in identifying securities, futures and leveraged foreign exchange businesses (hereinafter collectively referred to as “securities sector” or “securities businesses”) specific suspicious transactions.</i>
	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 legislative 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.
s.399(6) of SFO	1.8a	<i>A failure on the part of any person to comply with any provision of this Guideline shall not by itself render him liable to any judicial or other proceedings, but in any proceedings under the SFO before any court this Guideline shall be 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, it shall be taken into account in determining that question.</i>
s.193 & 194 of SFO	1.8b	<i>In addition, a failure to comply with any of the requirements of this Guideline by LCs and licensed representatives (where applicable) may reflect adversely on their fitness and properness and may be considered to be misconduct.</i>
s.193 & 196 of SFO	1.8c	<i>Similarly, a failure to comply with any of the requirements of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the Hong Kong Monetary Authority or to have regard to paragraphs 7.38 and 7.39 of this Guideline by RIs may reflect adversely on their fitness and properness and may be considered to be misconduct.</i>
The nature of money laundering and terrorist financing		
s.1, Sch. 1, AMLO	1.9	<p>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:</p> <ul style="list-style-type: none"> (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, <p>not to appear to be or so represent such proceeds.</p>
	1.10	<p>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:</p> <ul style="list-style-type: none"> (a) <u>Placement</u> - the physical disposal of cash proceeds derived from illegal activities; (b) <u>Layering</u> - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and (c) <u>Integration</u> - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.



Potential uses of the securities sector in the money laundering process

	1.10a	<i>Since the securities businesses are no longer predominantly cash based, they are less conducive to the initial placement of criminally derived funds than other financial industries, such as banking. Where, however, the payment underlying these transactions is in cash, the risk of these businesses being used as the placement facility cannot be ignored, and thus due diligence must be exercised.</i>
	1.10b	<i>The securities businesses are more likely to be used at the second stage of money laundering, i.e. the layering process. Unlike laundering via banking networks, these businesses provide a potential avenue which enables the launderer to dramatically alter the form of funds. Such alteration may not only allow conversion from cash in hand to cash on deposit, but also from money in whatever form to an entirely different asset or range of assets such as securities or futures contracts, and, given the liquidity of the markets in which these instruments are traded, with potentially great frequency.</i>
	1.10c	<i>Investments that are cash equivalents e.g. bearer bonds and similar investments in which ownership can be evidenced without reference to registration of identity, may be particularly attractive to the money launderer.</i>
	1.10d	<i>As mentioned, transactions in the securities sector may prove attractive to money launderers due to the liquidity of the reference markets. The combination of the ability to readily liquidate investment portfolios procured with both licit and illicit proceeds, the ability to conceal the source of the illicit proceeds, the availability of a vast array of possible investment mediums, and the ease with which transfers can be effected between them, offers money launderers attractive ways to effectively integrate criminal proceeds into the general economy.</i>
	1.10e	<i>The chart set out below illustrates the money laundering process relevant to the securities sector in detail.</i>



		<pre> graph TD A[Drugs cash Imports] --> B[CASH PROCEEDS FROM STREET SALES AND DRUGS CASH IMPORTS] B --> C[NET CASH PROCEEDS AFTER CASH OPERATING COSTS] C --> D[CASH DEPOSITS IN LEGITIMATE FINANCIAL INSTITUTION] C --> E[CASH PAYMENTS OF SECURITIES OR FUTURES / LEVERAGED FOREIGN EXCHANGE CONTRACTS OR INVESTMENT] D --> F[PURCHASE OF SECURITIES OR FUTURES / LEVERAGED FOREIGN EXCHANGE CONTRACTS] F --> G[SALE OF SECURITIES OR CLOSING OUT FUTURES / LEVERAGED FOREIGN EXCHANGE CONTRACTS OR SWITCH TO OTHER FORMS OF INVESTMENT] E --> H[PROCEEDS FROM SALE OF SECURITIES OR CLOSING OUT FUTURES / LEVERAGED FOREIGN EXCHANGE CONTRACTS OR INVESTMENT FOR OTHER LEGITIMATE USE] G --> H </pre> <p><i>Other examples of money laundering methods and characteristics of financial transactions that have been linked with terrorist financing can be found on the websites of the JFIU (www.jfiu.gov.hk) and FATF (www.fatf-gafi.org).</i></p>
s.1, Sch. 1, AMLO	1.11	<p>The term “terrorist financing” is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means:</p> <ul style="list-style-type: none"> (a) the provision or collection, by any means, directly or indirectly, of funds – <ul style="list-style-type: none"> (i) with the intention that the funds be used; or (ii) knowing that the funds will be used, in whole or in part, to commit one or more terrorist acts (whether or not the funds are actually so used); or (b) making available funds or financial (or related) services, 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.
	1.12	<p>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.</p>
Legislation concerned with money laundering and terrorist financing		
	1.13	<p>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</p>



		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”) ¹ 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 Crime 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.
AMLO		
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.
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 \$10,000,000 and 3 times the amount of profit gained, or costs avoided, by the FI as a result of the contravention.

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



<u>DTROP</u>		
	1.19	The DTROP contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction.
<u>OSCO</u>		
	1.20	<p>The OSCO, among other things:</p> <ul style="list-style-type: none"> (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.
<u>UNATMO</u>		
	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 funds and making funds or financial (or related) services available to terrorists or terrorist associates. The highest penalty for the offence upon conviction is imprisonment for 14 years and a fine. The UNATMO also permits terrorist property to be frozen and subsequently forfeited.
s.25A, DTROP & OSCO, s.12 & 14, UNATMO	1.24	The DTROP, the OSCO and the UNATMO also make it an offence if a person fails to disclose, as soon as it is reasonable for him to do so, his knowledge or suspicion of any property that directly or indirectly, represents a person's proceeds of, was used in connection with, or is intended to be used in connection with, drug trafficking, an indictable offence or is terrorist property respectively. This offence carries a maximum term of imprisonment of 3 months and a fine of \$50,000 upon conviction.
s.25A, DTROP & OSCO, s.12 & 14, UNATMO	1.25	"Tipping off" is another offence under the DTROP, the OSCO and the UNATMO. A person commits an offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.



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”).
	2.2	While no system will detect and prevent all ML/TF activities, FIs should assess the ML/TF risk in order to establish and implement adequate and appropriate AML/CFT systems (including customer acceptance policies and procedures) taking into account factors including products and services offered, types of customers, geographical locations involved.
	2.3	To ensure proper implementation of such policies and procedures, FIs should have effective controls covering: <ul style="list-style-type: none"> (a) senior management oversight; (b) appointment of a Compliance Officer (CO) and a Money Laundering Reporting Officer (MLRO)²; (c) compliance and audit function; and (d) staff screening and training³.

Risk factors

Product/service risk

	2.4	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

	2.5	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 agencies or intermediaries may also increase risk as the business relationship between the customer and an FI may become indirect.
--	-----	---

Customer risk

	2.6	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.
	2.7	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:

² The role and functions of an MLRO are detailed at paragraphs 7.18-7.29. For some FIs, the functions of the CO and the MLRO may be performed by the same staff member.

³ For further guidance on staff training see Chapter 9.



		<ul style="list-style-type: none"> (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. <p>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:</p> <ul style="list-style-type: none"> (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).
Senior management oversight		
	2.9	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.
	2.10	<p>Senior management should:</p> <ul style="list-style-type: none"> (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.
	2.11	<p>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:</p> <ul style="list-style-type: none"> (a) subject to constraint of size of the FI, independent of all operational and business functions; (b) normally resident 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;



		<p>(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</p> <p>(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 same status).</p>
<u>Compliance officer and money laundering reporting officer</u>		
	2.12	<p>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:</p> <p>(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</p> <p>(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.</p>
	2.13	<p>In order to effectively discharge these responsibilities, a number of areas should be considered. These include:</p> <p>(a) the means by which the AML/CFT systems are managed and tested;</p> <p>(b) the identification and rectification of deficiencies in the AML/CFT systems;</p> <p>(c) reporting numbers within the systems, both internally and disclosures to the Joint Financial Intelligence Unit (JFIU);</p> <p>(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;</p> <p>(e) the communication of key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies;</p> <p>(f) changes made or proposed in respect of new legislation, regulatory requirements or guidance;</p> <p>(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</p> <p>(h) AML/CFT staff training.</p>
	2.14	<p>The MLRO should play an active role in the identification and reporting of suspicious transactions. Principal functions performed are expected to include:</p> <p>(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;</p> <p>(b) maintaining all records related to such internal reviews;</p> <p>(c) providing guidance on how to avoid "tipping off" if any disclosure is made; and</p> <p>(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.</p>
<u>Compliance and audit function</u>		



	2.15	Where practicable, an FI should establish an independent compliance and audit function which is free of operating responsibilities. This function should have a direct line of communication to the senior management of the FI.
	2.16	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		
	2.17	FIs must establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new directors and employees.
Business conducted outside Hong Kong		
s.22(1), Sch. 2	2.18	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 ⁴ 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	2.19	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: <ul style="list-style-type: none"> (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	2.20	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 or the business relationship is managed in Hong Kong, reporting to the JFIU ⁵ may be required in such circumstances, but only if section 25A of OSCO/DTROP applies.

⁴ The FATF essential criteria 22.1 requires 'measures consistent with the home country requirements'.

⁵ 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	<p>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.</p> <p>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.</p>
--	-----	---

General requirement

	3.2	<p>FIs should determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer, the business relationship with that 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.</p> <p>The RBA will enable FIs to subject customers to proportionate controls and oversight by determining:</p> <ul style="list-style-type: none"> (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. <p>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.</p> <p>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.</p>
	3.3	<p>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.</p> <p>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.</p>

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, FIs are suggested to take the following factors into consideration when making the assessment: (i) country risk, (ii) customer risk, (iii) product/service risk and (iv)



	<p>delivery/distribution channel risk. For the avoidance of doubt, the examples provided are not exhaustive.</p> <p>1. Country risk</p> <p>Customers with residence in or connection with high-risk jurisdictions⁶ for example:</p> <ul style="list-style-type: none"> (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. <p>In assessing country risk associated with a customer, regard should be had 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.</p> <p>2. Customer risk</p> <p>The following are examples of customers who might be considered to carry lower ML/TF risks:</p> <ul style="list-style-type: none"> (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. <p>However, some customers, by their nature or behaviour might present a higher risk of ML/TF. Factors might include:</p> <ul style="list-style-type: none"> (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. <p>3. Product/service risk</p> <p>The products or services the customer is using should also be considered. Factors presenting higher risk might include:</p>
--	---

⁶ 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.



		<p>(a) services that inherently have provided more anonymity;</p> <p>(b) ability to pool underlying customers/funds; and</p> <p>(c) ability to use hold mail or mail forwarding facilities.</p> <p>4. Delivery / distribution channel risk</p> <p>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 agencies or intermediaries may also increase risk as the business relationship between the customer and an FI may become indirect.</p>
Ongoing review		
	3.6	<p>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 on-going 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.</p>
	3.7	<p>FI's should keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.</p>
Documenting risk assessment		
	3.8	<p>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:</p> <p>(a) how it assesses the customer's ML/TF risk; and</p> <p>(b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/TF risk.</p>



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 section 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	<p>The following measures are CDD measures applicable to an FI:</p> <ul style="list-style-type: none"> (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 trust⁷, 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: <ul style="list-style-type: none"> (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 not defined in the AMLO. Its meaning should be inferred from its everyday meaning and in the context of the industry practice.
	4.1.4a	<i>For the securities sector, the term 'customer' refers to a person who is a client of an LC and the term 'client' is as defined in section 1 of Part 1 of Schedule 1 to the SFO.</i>
	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

⁷ For the purpose of this guideline, a trust means an express trust or any similar arrangement (e.g.: foundation) for which a legal-binding document (i.e. a trust deed or in any other forms) is in place.



		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. ⁸
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 ⁹ : (i) equal to or exceeding an aggregate value of \$120,000, whether carried out in a single operation or several operations that appear to the FI to be linked; or (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 ¹⁰ ; 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.

⁸ It should be noted that 'occasional transactions' do not apply to the insurance and securities sectors.

⁹ Occasional transactions may include for example, wire transfers, currency exchanges, purchase of cashier orders or gift cheques.

¹⁰ This criterion applies irrespective of the \$120,000 threshold.



4.2 Identification and verification of the customer's identity		
s.2(1)(a), Sch. 2	4.2.1	<p>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:</p> <ul style="list-style-type: none"> (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 source¹¹ 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. In respect of a customer who is an individual (i.e. a natural person who is not acting in an official capacity on behalf of a legal person or trust), the customer himself is normally the beneficial owner. However, FIs should still ask whether the customer is acting on behalf of another person.
	4.3.2	Where an individual is identified as a beneficial owner, the FI should endeavour to obtain the same identification information (as for an individual customer) about that beneficial owner, in case this is not possible, at least the individual's name, nationality, date of birth and address.
	4.3.3	The verification requirements under the AMLO are, however, different for a customer and a beneficial owner.
	4.3.4	The obligation to verify the identity of a beneficial owner is for the FI to take reasonable measures, based on its assessment of the ML/TF risks, so that it is satisfied that it knows who the beneficial owner is.
s.1 & s.2(2), Sch. 2	4.3.5	FIs should identify all beneficial owners of a customer. In relation to verification of beneficial owners' identities, except where a situation referred to in section 15 of Schedule 2 exists ('high risk'), the AMLO requires FIs to take reasonable measures to verify the identity of any beneficial owners owning or controlling 25% or more of the voting rights or shares, etc. of a corporation, partnership or trust. In high risk situations referred to in section 15 of Schedule 2, the threshold for the requirement is 10%. ¹²
	4.3.6	In the case of trusts, the beneficiaries may be defined as a class of persons who may benefit from the trust. Where only a class of persons is available for identification, the FI should ascertain and name the scope of the class (e.g. children of a named individual) and measures should be put in place to facilitate the verification of the identity of these individuals when the FI becomes aware of any payment out of the trust account made to the beneficiaries.
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	<p>If a person purports to act on behalf of the customer, FIs must:</p> <ul style="list-style-type: none"> (i) identify the person and take reasonable measures to verify the person's identity

¹¹ See Appendix A.

¹² In circumstances where an existing customer is reclassified as high-risk under section 15 of Schedule 2, FIs may consider delaying taking reasonable measures to verify the beneficial owner's identity according to the enhanced threshold (i.e. remediate from 25% to 10%) where a risk of tipping-off exists.



		<p>on the basis of documents, data or information provided by-</p> <ul style="list-style-type: none"> (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 <p>(ii) verify the person's authority to act on behalf of the customer.</p>
s.2(1)(d), Sch. 2	4.4.2	FIs should obtain written authority (e.g. the board resolution or similar power of attorney) to verify that the individual purporting to represent the customer is authorized to do so.
	4.4.3	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 verify the identity of those authorized to give instructions for the movement of funds or assets.
4.5 Characteristics and evidence of identity		
	4.5.1	<p>It should be appreciated that 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.</p> <p>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. Appropriate steps would include ensuring that staff assessing such documents are proficient in the language or obtaining a translation from a suitably qualified person.</p>
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	<p>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:</p> <ul style="list-style-type: none"> (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, for example by obtaining copies of recent and current statements.



	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 satisfy itself, that there is a bona-fide rationale for a non-resident to seek to establish a business relationship in Hong Kong. Based on its risk assessment, the FI should also consider subjecting accounts maintained by non-residents to EDD and enhanced monitoring.
4.7 Timing of identification and verification of identity		
<u>General requirement</u>		
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.
<u>Delayed identity verification during the establishment of a business relationship</u>		
	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: <ul style="list-style-type: none"> (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: <ul style="list-style-type: none"> (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 policyholder 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.
	4.7.6	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:



		<ul style="list-style-type: none"> (a) establishing timeframes for the completion of the identity verification measures; (b) requiring senior management to monitor such relationships pending completion of the identity verification; (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, (other than to invest or deposit funds on behalf of the customer until identity verification is completed). Exceptions¹³ may be made to allow payments to third parties subject to the following conditions: <ul style="list-style-type: none"> (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	<p>The FI must not use this concession for the circumvention of CDD procedures, in particular, where it:</p> <ul style="list-style-type: none"> (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	<p>Verification of identity should be concluded within a reasonable timeframe. 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:</p> <ul style="list-style-type: none"> (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 days¹⁴ 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,	4.7.9	<p>The FI should assess whether this failure provides grounds for knowledge or suspicion of ML/TF and a report to the JFIU is appropriate.</p>

¹³ It should be noted that the exceptions do not apply to insurance sector.

¹⁴ For address proof, this period may be extended to 90 working days.



UNATMO		
	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	<p>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.</p> <p>An appropriate time to do so is upon certain trigger events. These include:</p> <ul style="list-style-type: none"> (a) when a significant transaction¹⁵ is to take place; (b) when a material change¹⁶ occurs in the way the customer’s account is operated,¹⁷; (c) when the FI’s customer documentation standards change substantially; or (d) when the FI is aware that it lacks sufficient information about the customer concerned. <p>In all cases, the factors determining the period of review or what constitutes a trigger event should be clearly defined in the FI’s policy and procedures.</p>
	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 policy and procedures.
4.8 Natural Persons		
Identification		
s.2 & 3, Sch. 2	4.8.1	<p>FIs should collect the following identification information in respect of personal customers and other natural persons, including connected parties of a legal person, who need to be identified:</p> <ul style="list-style-type: none"> (a) legal name, any former names and any other names used; (b) residential address (and permanent address if different); (c) date of birth;

¹⁵ 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.

¹⁶ For example, an existing customer applying to open a new account may constitute a material change.

¹⁷ Reference should also be made to section 6 of Schedule 2 ‘Provisions relating to Pre-Existing Customers’.



		(d) nationality; and (e) 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 the individual's identity, including name, date of birth, identity card number by reference to their Hong Kong identity card. FIs should verify 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 'biadata' 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 verification		
	4.8.8	An FI should verify the address 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	FIs may adopt a risk-based approach to determine the need to verify the address of a beneficial owner, other relevant individuals associated with the relationship or transaction, connected parties and occasional customers. Where the obligation to verify the address of these parties arises, the FI should take reasonable measures to verify the address of these parties, taking account of the number of individuals, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship between them.
	4.8.10	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.
	4.8.11	<p>Methods for verifying residential addresses may include obtaining:</p> <ul style="list-style-type: none"> (a) a recent utility bill (except mobile telephone bills, as such service has no connection to the registered address) issued within the last 3 months; (b) recent correspondence from a Government department or agency (i.e. issued within the last 3 months); (c) bank statements, issued by an authorised institution within the last 3 months; (d) a record of a personal visit to the residential address by a staff member of the FI; (e) 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); (f) 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; (g) 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; (h) a Hong Kong tenancy agreement which has been duly stamped by the Inland Revenue Department; (i) a current Hong Kong domestic helper employment contract (I.D 407) stamped by an appropriate Consulate and the name of the employer should correspond with the applicant's visa endorsement in their passport; (j) a letter from a Hong Kong employer together with proof of employment, which an FI is satisfied that it can place reliance on, that confirms residence at a stated address in Hong Kong, and indicates the expected duration of employment. In the case of a migrant worker, details of the worker's principal residential address in their country of origin should also be recorded; (k) a lawyer's confirmation of property purchase, or legal document recognising title to property; (l) 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; and (m) for non-Hong Kong residents, independent overseas electronic data sources, e.g. a search of the relevant electoral register (for high-risk relationships and transactions, performing (m) alone is not sufficient).
	4.8.12	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



		<p>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).</p> <p>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.</p>
Other considerations		
	4.8.13	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.
	4.8.14	Appendix A contains a list of documents recognised by the RAs as independent and reliable sources for identity verification purposes.
4.9 Legal Persons		
General		
	4.9.1	This section of the Guideline details the measures FIs should take when establishing a business relationship, or performing an occasional transaction above the specified thresholds, whether it is a single operation or a series of operations, for customers other than natural persons.
	4.9.2	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	4.9.3	In deciding who the beneficial owner is in relation to a legal person (i.e. 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.
	4.9.4	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	4.9.5	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	4.9.6	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.
	4.9.7	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, is not independently verified.
Corporation		
<i>Identification information</i>		
	4.9.8	<p>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.</p> <p>An FI should obtain and verify the following information in relation to a customer which is a corporation:</p> <ul style="list-style-type: none"> (a) full name; (b) date and place of incorporation; (c) registration or incorporation number; and (d) registered office address in the place of incorporation and address of principal place of business/operations (if different from registered office).
	4.9.9	<p>In the course of verifying the customer's information mentioned in paragraph 4.9.8, an FI should also obtain the following information¹⁸:</p> <ul style="list-style-type: none"> (a) a copy of the certificate of incorporation or registration issued by the company registry in the jurisdiction of incorporation; (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.
s.2(1)(d), Sch. 2	4.9.10	FIs should obtain the board resolution or similar written authority (e.g. power of attorney) to verify that the individual purporting to represent the corporation is authorized to do so, in addition to recording and taking reasonable measures to verify the identity of that individual.
	4.9.11	<p>An FI should also:</p> <ul style="list-style-type: none"> (a) identify and record the identity of all directors and verify the identity of at least one director. Following the FI's assessment of the ML/TF risks presented by the

¹⁸ Examples given are not exhaustive.



		<p>company, it may decide to verify the identity of additional directors as appropriate, in accordance with the guidance for individuals; and</p> <p>(b) identify and record the identity of all beneficial owners, and take reasonable measures to verify the identity of:</p> <ul style="list-style-type: none"> (i) all shareholders holding 25% (for normal risk circumstances) / 10% (for high risk circumstances) or more of the voting rights or share capital; (ii) any individual who exercises ultimate control over the management of the corporation; and (iii) any person on whose behalf the customer is acting.
	4.9.12	<p>FIs should perform a company registry search and obtain a full company search report¹⁹ in respect of all locally incorporated private (i.e. non-listed) companies and companies incorporated in jurisdictions which have a public company registry to:</p> <ul style="list-style-type: none"> (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.
	4.9.13	<p>In respect of a company incorporated in a jurisdiction that does not have a public company registry (e.g. British Virgin Islands) or has only a partially public registry (e.g. Bermuda), a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation should be obtained²⁰.</p>
Beneficial owners		
s.1, Sch.2	4.9.14	<p>The AMLO defines beneficial owner in relation to a corporation as:</p> <ul style="list-style-type: none"> (i) an individual who – <ul style="list-style-type: none"> (a) owns or controls, directly or indirectly, including through a trust or bearer share holding, not less than 10% of the issued share capital of the corporation; (b) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights at general meetings of the corporation; or (c) exercises ultimate control over the management of the corporation; r (ii) if the corporation is acting on behalf of another person, means the other person.
	4.9.15	<p>For companies with multiple layers in their ownership structures, an FI may demonstrate that it has an understanding of the ownership and control structure of the company and has fully identified the intermediate layers by obtaining a director's declaration incorporating or annexing an ownership chart describing the intermediate layers (e.g. company name, place of incorporation, incorporation number, date of incorporation, etc.). The director's declaration should also fully identify the beneficial owners and detail the rationale behind the particular structure employed.</p>
	4.9.16	<p>While 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 (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</p>

¹⁹ Alternatively, the FI may obtain from the customer a certified true copy of a full company search report.

²⁰ FIs may accept certified true copy of certificate of incumbency that is issued within 6 months.



		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.
<i>Persons purporting to act on behalf of the customer</i>		
s.2(1)(d), Sch. 2	4.9.19	<p>Section 2(1)(d) of Schedule 2 requires FIs to identify and take reasonable measures to verify the identity of persons purporting to act on behalf of customers²¹ (e.g. authorized account signatories). The basic requirement is therefore to verify the identity of such persons by reference to the documents and other means listed in Appendix A wherever possible.</p> <p>According to section 2(1)(d)(i) of Schedule 2, FIs should identify the person and take reasonable measures to verify the person's identity based on documents, data or information provided for in section 2(1)(d)(i)(A) to (C) of Schedule 2, or any other reliable and independent source that is recognized by the RA. FIs may on occasion encounter difficulties in verifying all signatories of customers such as listed companies that may have very long lists of authorized 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 verify the person's identity. For example, in respect of verification of account signatories related to a customer which is an FI or a listed company²², and the risk is considered as low, FIs could adopt a more streamlined approach in verifying the identities of the account signatories. The adoption of a signatory list, in which the identities of the account signatories have been verified by a department or person within that FI or listed company, which is independent to the persons whose identities are being verified (e.g. compliance, audit or human resources) may be sufficient to demonstrate reasonable measures.</p> <p>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.</p>
<u>Partnerships and unincorporated bodies</u>		
	4.9.20	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.

²¹ This only applies to persons who are able to give instructions concerning transfer of funds or assets belonging to the customer.

²² Having regard to the advice provided at paragraphs 4.15.



s.1, Sch. 2	4.9.21	<p>The AMLO defines beneficial owner, in relation to a partnership as:</p> <ul style="list-style-type: none"> (i) an individual who <ul style="list-style-type: none"> (a) is entitled to or controls, directly or indirectly, not less than a 10% share of the capital or profits of the partnership; (b) is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% 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	4.9.22	<p>In relation to an unincorporated body other than a partnership, beneficial owner:</p> <ul style="list-style-type: none"> (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.
	4.9.23	<p>The FI should obtain the following information in relation to the partnership or unincorporated body:</p> <ul style="list-style-type: none"> (a) the full name; (b) the business address; and (c) the names of all partners/principals who exercise control over the management of the partnership or unincorporated body, and names of individuals who own or control not less than 10% of its capital or profits, or of its voting rights. <p>In cases where a formal 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.</p>
	4.9.24	<p>When establishing a business relationship with a partnership or unincorporated body operating a business in Hong Kong, FIs should verify the identity of the registered owners and operators.</p>
	4.9.25	<p>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/principals 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 of the partnerships or unincorporated bodies.</p>
	4.9.26	<p>Other partnerships and unincorporated bodies have a lower profile, and generally comprise a much smaller number of partners/principals. In verifying the identity of such customers, FIs should primarily have regard to the number of partners/principals. 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.</p>



	4.9.27	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.
<u>Trusts</u>		
<i>General</i>		
	4.9.28	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	4.9.29	<p>The AMLO defines the beneficial owner, in relation to a trust as:</p> <ul style="list-style-type: none"> (i) an individual who is entitled to a vested interest in not less than 10% of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; (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 (this would include the trustee in situations where the trustee is not the direct customer).
	4.9.30	<p>FIs should collect the following identification information in respect of a trust on whose behalf the trustee (i.e. the customer) is acting:</p> <ul style="list-style-type: none"> (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) (including initial settlors and persons subsequent settling funds into the trust) and any protector(s) or enforcers in line with the guidance for individuals/corporations; and (g) identification information of known beneficiaries. 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.
<i>Verifying the trust and placing reliance on the trustees</i>		
	4.9.31	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 and measures should be put in place to facilitate the verification of their identity at the time when the FI becomes aware of the distribution



		<p>of trust property. 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.</p> <p>Verification of the existence, legal form and parties to a trust should therefore, wherever possible, be conducted by means of reviewing a copy of the trust instrument. In such circumstances, a redacted copy should be retained on file to evidence the existence and parties to the trust. Where this is not reasonably available, reasonable measures to verify this information, having regard to the ML/TF risk, may include :</p> <p>(a) a written declaration/confirmation from a trustee acting in a professional capacity²³; or</p> <p>(b) a written declaration/confirmation from a lawyer who has reviewed the relevant instrument.</p> <p>The person mentioned in (a) and (b) above should fulfil the requirements of section 18(3) of Schedule 2.</p> <p>For the avoidance of doubt, reasonable measures are still required to be taken to verify the actual identity of the individual parties (i.e. trustee, settlor, protector, beneficiary, etc.).</p>
	4.9.32	An FI should verify the identity of the beneficiaries when the FI becomes aware of any payment out of the trust account made to the beneficiaries . This includes where payments are made directly to beneficiaries and when payments are made to the trustees. In the latter case, FIs should establish whether the payment is intended for a beneficiary of a trust and if so obtain verification documents.
	4.9.33	Particular care should be taken in relation to trusts created in jurisdictions where there is no money laundering legislation similar to Hong Kong.
<i>Other considerations</i>		
	4.9.34	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)		
<u>General</u>		
	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. However, other aspects of CDD must be undertaken and it is 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	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

²³ "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).



2.		the customer, the product, and account type falls within paragraphs 4.10.3, 4.10.16 and 4.10.18 below.
s.4(3), Sch 2.	4.10.3	<p>The AMLO defines customers to whom SDD may be applied as follows:</p> <ul style="list-style-type: none"> (a) an FI as defined in the AMLO; (b) an institution that- <ul style="list-style-type: none"> (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- <ul style="list-style-type: none"> (i) an FI; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that- <ul style="list-style-type: none"> 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	<p>For avoidance of doubt, the FI must still:</p> <ul style="list-style-type: none"> (a) identify the customer and verify 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, <ul style="list-style-type: none"> (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, <p>in accordance with the relevant requirements stipulated in this Guideline.</p>
Local and foreign financial institution		
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 in the name of a nominee company for holding fund units on behalf of the second-mentioned FI or the underlying customers of the fund, provided that the second-mentioned FI has conducted CDD on the underlying customers and is authorised 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.
<u>Listed company</u>		
s.4(3)(c), Sch. 2	4.10.8	FIs may perform SDD in respect of a corporate customer listed on a stock exchange ²⁴ . This means FIs need not identify the beneficial owners of the listed company. In all other cases, FIs should follow the CDD requirements for a legal person set out in paragraphs 4.9 of this Guideline.
	4.10.9	FIs should identify and record the identities of all directors. FIs may adopt a risk-based approach in determining whether it is necessary to verify the identity of any of the directors of a listed company.
<u>Investment vehicle</u>		
s.4(3)(d), Sch. 2	4.10.10	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.
	4.10.11	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.
	4.10.12	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 trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the CDD. Where the person responsible for carrying out the CDD measures (the investment vehicle 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 set out in the Schedule 2.
	4.10.13	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 not less than 10% interest of the investment vehicle. Except where the investment vehicle is being operated for "private" use by a specific group of persons, the FI may, if it considers it appropriate to do so under its risk-based approach, 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. Where the FI accepts such a representation, this should be documented, retained, and subject

²⁴ Reference should be made to paragraphs 4.15.



		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	4.10.14	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	4.10.15	Public body includes: <ul style="list-style-type: none"> (a) any executive, legislative, municipal or urban council; (b) any Government department or undertaking; (c) any local or public authority or undertaking; (d) any board, commission, committee or other body, whether paid or unpaid, appointed by the Chief Executive or the Government; and (e) any board, commission, committee or other body that has power to act in a public capacity under or for the purposes of any enactment.
SDD in relation to specific products		
s.4(4) & (5), Sch. 2	4.10.16	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: <ul style="list-style-type: none"> (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: <ul style="list-style-type: none"> (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.
	4.10.17	For the purpose of item (a) of paragraph 4.10.16, FIs may treat the employer, the trustee and any other person who has control over the business relationship including the administrator or the scheme manager, as the customer. FIs are not required to apply the provisions of section 2(1)(b) of Schedule 2 where the customer is a scheme falling within item (a) of paragraph 4.10.16. This means that they need not normally identify the beneficial owners of the scheme, i.e. the employees and verify their identities. It is only necessary to conduct CDD on the customer of the FI.
Solicitor's client accounts		
s.4(6), Sch. 2	4.10.18	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: <ul style="list-style-type: none"> (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.
	4.10.19	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.
	4.10.20	FI should obtain evidence to satisfy that the solicitor is authorized to practise in Hong Kong under the Legal Practitioners Ordinance (Cap. 159). 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.
	4.10.21	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	<p>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. Examples of higher risk customers may include, having regard to the identified ML/TF risks:</p> <ul style="list-style-type: none"> (a) non-resident customers; (b) private banking; (c) legal persons or arrangements such as trusts that are personal assets holding vehicles; and (d) companies that have nominee shareholders or shares in bearer form. <p>Additional measures²⁵ or EDD should be taken to mitigate the ML/TF risk involved, which for illustration purposes, may include:</p> <ul style="list-style-type: none"> (a) obtaining additional information on the customer (e.g. connected 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.
4.12 Customer not physically present for identification purposes		
	4.12.1	FIs must apply equally effective customer identification procedures and on-going monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview. 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

²⁵ Additional measures should be documented in the FI's policy and procedures.



		customer they are dealing with. Consequently, there are increased risks.
s.5(3)(a) & s.9, Sch. 2	4.12.2	<p>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:</p> <ul style="list-style-type: none"> (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 all the information provided by the customer; (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. <p>Measures which would meet the requirements of paragraph 4.12.2(a) and (b) above include obtaining copies of documents that have been certified by a suitable certifier.</p>
	4.12.2a	<i>In taking additional measures to mitigate the risks posed by customers not physically present for identification purposes, reference should be made by LCs to the relevant provisions (presently paragraph 5.1) in the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission concerning account opening procedures for customers who are not physically present for identification purposes.</i>
<u>Suitable certifiers and the certification procedure</u>		
	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.
s.18, Sch. 2	4.12.4	<p>Suitable persons to certify verification of identity documents may include:</p> <ul style="list-style-type: none"> (a) an intermediary specified in section 18(3) of Schedule 2; (b) a member of the judiciary in an equivalent jurisdiction; (c) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; 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 and provide his/her contact details. The certifier must state that it is a true copy of the original (or words to similar effect).
	4.12.6	<p>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.</p> <p>In any circumstances where an FI is unsure of the authenticity of certified</p>



		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)		
<u>Background</u>		
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, 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.
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	<p>A politically exposed person is defined in the AMLO as:</p> <ul style="list-style-type: none"> (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 <ul style="list-style-type: none"> (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	<p>The AMLO defines a close associate as:</p> <ul style="list-style-type: none"> (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 first-mentioned individual 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	<p>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 the Transparency International Corruption Perceptions Index, which ranks countries according to their perceived level of corruption).</p> <p>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.</p>
s.5(3)(b) & s.10, Sch. 2	4.13.11	<p>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:</p> <ul style="list-style-type: none"> (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.
<i>Senior management approval</i>		
	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 in the same manner as PEP, except the individual will have been entrusted with a prominent public function within the People's Republic of China or be a family member or close associate of such an individual.
	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 relevant and up-to-date.
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	FIs should review the memorandum and articles of association to ascertain whether the company has the capacity to issue such shares.
	4.14.4	It is a best practice for FIs to understand each jurisdiction's requirements and practices in respect of bearer shares. For example, a number of jurisdictions require bearer shares to be deposited with a registered custodian (e.g. the British Virgin Islands, the Cayman Islands). This information is available publicly or for easier reference may be sourced in consolidated form, an example of which is OECD's annual report on tax co-operation, which provides a breakdown of each jurisdiction's requirements in respect of bearer shares.



	4.14.5	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.
	4.14.6	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 holding 10% or more of the share capital. Given the higher ML/ TF risks associated with bearer shares, FIs may wish to adopt higher levels of risk mitigation than prescribed in the AMLO and obtain such declarations from each beneficial owner holding 5% or more of the share capital. 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	<p>FIs should give particular attention to, and exercise extra care in respect of:</p> <ul style="list-style-type: none"> (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. <p>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 be fully satisfied with the legitimacy of the source of funds of such customers.</p>
	4.15.2	<p>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:</p> <ul style="list-style-type: none"> (a) circulars issued to FIs by RAs; (b) whether the jurisdiction is or a significant number of persons or entities in that jurisdiction are, 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. <p>"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</p>



		<p>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.</p> <p>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.</p> <p>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 equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong.</p>
4.16 Notice in writing from an RA		
s.15, Sch. 2	4.16.1	<p>Where the requirement is called for by the FATF (which may include mandatory EDD or the application of countermeasures²⁶) or in other circumstances independent of the FATF but also considered to be higher risk, RA may, through a notice in writing:</p> <ul style="list-style-type: none"> (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. <p>The type of EDD / countermeasures would be proportionate to the nature of the risks and/or deficiencies.</p>
4.17 Reliance on CDD performed by intermediaries		
<u>General</u>		
s.18, Sch. 2	4.17.1	<p>FIs may rely upon an intermediary to perform any part of the CDD measures 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.</p> <p>For avoidance of doubt, reliance on intermediaries does not apply to:</p> <ul style="list-style-type: none"> (a) outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the FI to carry out its CDD function. In such a situation the outsource or agent is to be regarded as synonymous with the FI (i.e. the processes and documentation are those of the FI itself); and (b) business relationships, accounts or transactions between FIs for their clients. <p>In practice, this reliance on third parties often occurs through introductions made by another member of the same financial services group, or in some jurisdictions from another FI or third party.</p>
s.18(1) &	4.17.2	The FI must obtain written confirmation from the intermediary that:

²⁶ 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. .



s.18(4)(b), Sch. 2		<p>(a) it agrees to perform the role; and</p> <p>(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.</p> <p>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.</p>
	4.17.3	FIs should obtain satisfactory evidence to confirm the status and eligibility of the intermediary. Such evidence may comprise corroboration from the intermediary's regulatory authority, or evidence from the intermediary of its status, regulation, policies and procedures.
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 six 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. FIs 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	FIs 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)(b), Sch. 2	4.17.8	FIs may rely upon an authorized institution, a licensed corporation, an authorised insurer, an appointed insurance agent or an authorised insurance broker, to perform any part of the CDD measures.
s.18(3)(a), Sch. 2	4.17.9	<p>FIs may also rely upon the following categories of domestic intermediaries:</p> <p>(a) a solicitor practising in Hong Kong;</p> <p>(b) a certified public accountant practising in Hong Kong;</p> <p>(c) a current member of The Hong Kong Institute of Chartered Secretaries</p>



s. 18(5), Sch. 2		<p>practising in Hong Kong; and</p> <p>(d) a trust company registered under Part VIII of the Trustees Ordinance carrying on trust business in Hong Kong,</p> <p>provided that the intermediary is able to satisfy the FI that they have adequate procedures in place to prevent ML/TF.</p> <p>The arrangement for allowing FIs to rely on these intermediaries, which are not regulated under the AMLO for AML/CFT compliance, will expire three years after commencement of the AMLO.</p>
Overseas intermediaries		
18(3)(c), Sch. 2	4.17.10	<p>FIs may only rely upon an overseas intermediary carrying on business or practising in an equivalent jurisdiction where the intermediary:</p> <ul style="list-style-type: none"> (a) falls into one of the following categories of businesses or professions: <ul style="list-style-type: none"> (i) an institution that carries on a business similar to that carried on by an FI mentioned in paragraph 4.17.8; (ii) a lawyer or a notary public; (iii) an auditor, a professional accountant, or a tax advisor; (iv) a trust or company service provider; and (v) a trust company carrying on trust business; (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.
	4.17.11	<p>Compliance with the requirements set out above for both domestic or overseas intermediaries may entail the FI:</p> <ul style="list-style-type: none"> (a) reviewing the intermediary's AML/CFT policies and procedures; (b) making enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited; or (c) seeking an independent review of the intermediary's procedures by external auditors or other experts.
4.18 Pre-existing customers		
<u>Application of AMLO and guideline to pre-existing customers</u>		
s.6, Sch. 2	4.18.1	<p>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:</p> <ul style="list-style-type: none"> (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 will need to consider other trigger events specific to their own customers and business.
s.5, Sch. 2	4.18.3	FIs should note that requirements for on-going 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 keep 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		
<u>General</u>		
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 that are incorporated or established in an equivalent jurisdiction and section 18 of Schedule 2 restricts reliance upon intermediaries outside Hong Kong for CDD measures to those practising or carrying on business 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.
<u>Determination of jurisdictional equivalence</u>		
	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;



		<ul style="list-style-type: none">(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 the Transparency International 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	<p>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 relevant and up-to-date 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.</p>



Chapter 5 - ONGOING MONITORING

General

s.5(1), Sch. 2	5.1	<p>Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of an effective AML/CFT systems. It helps FIs to know their customers and to detect unusual or suspicious activities.</p> <p>An FI must continuously monitor its business relationship with a customer by:</p> <ul style="list-style-type: none"> (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; (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	<p>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.</p>
	5.3	<p>Possible characteristics FIs should consider monitoring include:</p> <ul style="list-style-type: none"> (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	<p>FIs should be vigilant for changes on the basis of the business relationship with the customer over time. These may include where:</p> <ul style="list-style-type: none"> (a) new products or services that pose higher risk are entered into; (b) new corporate or trust structures are created; (c) a change in a customer's employment or other circumstances takes place; (d) the stated activity or turnover of a customer changes or increases; or (e) the nature of transactions changes or their volume or size increases etc.
	5.5	<p>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.</p>
	5.6	<p>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.</p>



	5.7	FIs should ensure that any information obtained through meetings, discussions, or other methods of communication with the customer that is material to the updating of CDD records required under sections 2 and 3 of Schedule 2 is recorded and retained with the customer's records.
Risk-based approach to monitoring		
	5.8	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	5.9	<p>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, an FI should:</p> <ul style="list-style-type: none"> (a) determine whether it has adequate procedures or management information systems 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; (b) determine how it will monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded; and (c) conduct an annual independent review of CDD information, activities and transactions.
Methods and procedures		
	5.10	<p>When considering how best to monitor customer transactions and activities, an FI should take into account the following factors:</p> <ul style="list-style-type: none"> (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). <p>The methods to be considered include:</p> <ul style="list-style-type: none"> (i) exception reports to advise supervisors/operations managers of large transactions for their review; (ii) exception reports to advise the CO, MLRO or other appropriate staff, of customers and transactions meeting certain predetermined criteria; and (iii) computerised transaction monitoring systems.
s.5(1)(c), Sch. 2	5.11	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	5.12	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 : < http://www.jfiu.gov.hk/eng/suspicious_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.
	5.13	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 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 funds 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 funds is what matters. In terrorist financing, the focus is on the destination or use of funds, which may have derived from legitimate sources.
UNSCR 1373 (2001)	6.8	The UN Security Council has passed United Nations Security Council 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/Docs/sc/committees/1373/ .
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 funds or financial services available to or for the benefit of a terrorist or terrorist associate except under the authority of a licence granted by S for S. 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, in the absence of a licence granted by S for S, from making available, directly or indirectly, any funds 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.
s.6(1), UNATMO	6.15	The S for S can licence exceptions to the prohibitions to enable frozen funds 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(CP S)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	<p>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.</p> <p>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.</p>
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 a policy and procedure 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: <ul style="list-style-type: none"> (a) screening all 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	Where an FI freezes funds under Hong Kong's financial sanctions legislation or where it has suspicions of terrorist financing or sanction violations, it must make a report to the JFIU. If an FI suspects that a transaction is terrorist-related, it should also 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 is subject to and is liable for 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: <ul style="list-style-type: none"> (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(5), DTROP & OSCO, s.12(5), UNATMO	7.3	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.
	7.4	Once knowledge or suspicion has been formed the following general principles should be applied: <ul style="list-style-type: none"> (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 FI²⁷; (b) disclosures must be made as soon as is reasonably practical after the 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.
	7.5	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.
	7.6	FIs must ensure sufficient guidance is given to staff ²⁸ 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

²⁷ The reporting obligations require a person to report suspicions of ML/TF, irrespective of the amount involved. The reporting obligations of s25A(1) DTROP and OSCO and s12(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.

²⁸ In the context of Chapter 7, staff includes appointed insurance agents.



		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		
	7.7	<p>FIs have an obligation to report where there is knowledge or suspicion of ML/TF. Generally speaking, knowledge is likely to include:</p> <ul style="list-style-type: none"> (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.
	7.8	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence.
	7.9	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.
	7.10	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	7.11	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 : < http://www.jfiu.gov.hk/eng/suspicious_ask.html >).
	7.12	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.
	7.13	<p>The following is a (non-exhaustive) list of examples of situations that might give rise to suspicion in certain circumstances:</p> <ul style="list-style-type: none"> (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



		<p>reasonable explanation;</p> <p>(g) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;</p> <p>(h) transfers to and from high risk jurisdictions²⁹ without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and</p> <p>(i) unnecessary routing of funds or other property from/to third parties or through third party accounts.</p> <p>Further examples of what might constitute suspicious transactions are provided in paragraphs 7.38-7.39. 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 paragraphs 7.38-7.39 should prompt further investigations and be a catalyst towards making at least initial enquiries about the source of funds.</p> <p>FIs should also be aware of elements of individual transactions that could indicate funds involved in terrorist financing. The FATF has issued guidance for FIs in detecting terrorist financing³⁰. 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.</p>
	7.14	<p>The OSCO, DTROP and UNATMO prohibit FIs, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the JFIU. 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.</p> <p>The customer's awareness of a possible STR or investigation could compromise 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.</p>
Timing and manner of reports		
	7.15	<p>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 practicable³¹. The use of a standard form or the use of the e-channel 'STREAMS'³² by registered users is strongly encouraged. Further details of reporting methods and advice may be found at www.jfiu.police.gov.hk. In the event that an urgent disclosure is required, particularly when the account is part of an on-going 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.</p>
	7.16	<p>Disclosures can be made either before a suspicious transaction or activity occurs in circumstances where an intended transaction appears suspicious (whether the intended transaction ultimately takes place or not), or after a transaction or activity</p>

²⁹ Guidance on determining high risk jurisdictions is provided at paragraphs 4.15.

³⁰ Available on the FATF website at <http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf>.

³¹ 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.

³² 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.



		has been completed if the transaction appears suspicious only with the benefit of hindsight. Disclosures that are made after the activity or transaction has taken place are not intended as alternatives to reports that should have been made prior to the transaction or activity being processed or completed.
s.25A(1), DTROP & OSCO, s.12(1), UNATMO	7.17	FIs must make the submission of a disclosure a priority, whilst at the same time ensuring that the disclosure itself is comprehensive and meaningful. 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 the case of significant movement of funds or other property or the collection of cash, FIs should contact the JFIU urgently, before funds or the other property are/is moved or cash is collected.
Internal reporting		
	7.18	An FI should appoint a Money Laundering Reporting Officer (MLRO) as a central reference point for reporting suspicious transactions. More generally, the MLRO should have the responsibility of checking on an ongoing basis that the FI 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.
	7.19	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 & OSCO, s12(4), UNATMO	7.20	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 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 should 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.
	7.21	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.
	7.22	FIs should establish and maintain procedures to ensure that: <ul style="list-style-type: none"> (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.
	7.23	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 practicable, 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.
	7.24	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), UNATMO	7.25	The MLRO must acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries i.e. tipping off the customer or any other third party. The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU.
	7.26	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.
	7.27	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: <ul style="list-style-type: none"> (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 JFIU³³.
	7.28	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 not delay making a report to the JFIU. MLROs should document the evaluation process that they follow in each case and their reasons for their conclusions.
	7.29	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 practicable 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 a suspicious transaction report 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.
Recording internal reports		
	7.30	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

³³ For details, please see www.jfiu.gov.hk



		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		
	7.31	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		
	7.32	<p>FIs should note that:</p> <ul style="list-style-type: none"> (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	7.33	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.
	7.34	Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and Customs Excise Department recognise the importance



		of having effective feedback procedures in place. The JFIU provides feedback both in its quarterly report ³⁴ and upon request, to a disclosing FI in relation to the current status of an investigation.
	7.35	After initial analysis by the JFIU, reports that are to be developed are allocated to financial investigation officers for further investigation. Where additional information is required from a reporting institution following a suspicious transaction report, it will be obtained pursuant to a search warrant or production order. 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	7.36	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.
s.3, DTROP, s.8, OSCO, s.13, UNATMO	7.37	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.
ML through the securities sector		
<i>ML using transactions involving securities, futures contracts or leveraged foreign exchange contracts</i>		
	7.38	<p>Customer-related</p> <p>(a) A customer introduced by an overseas bank, affiliate or other investor both of which are based in jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise pose higher risk.</p> <p>(b) A foreign based customer who uses domestic accounts to trade on foreign stock / futures exchanges.</p> <p>(c) Requests by customers for investment management services (as regards securities, futures contracts or leveraged foreign exchange contracts) where the source of the funds is unclear or not consistent with the customers' apparent standing.</p> <p>(d) A customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.</p> <p>Trading-related</p> <p>(a) Buying and selling of securities/futures with no discernible purpose or where the nature, size or frequency of the transactions appears unusual. For example,</p>

³⁴ 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 STR's 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.



		<p>where a customer frequently purchases securities at a high price and subsequently sells them at a considerable loss to the same party. This may indicate transferring value from one party to another.</p> <p>(b) A number of transactions by the same customer in small amounts relating to the same investment, each purchased for cash and then sold in one transaction, the proceeds being paid to a person other than that customer.</p> <p>(c) A customer engages in prearranged or other non-competitive trading in particular securities, futures contracts or leveraged foreign exchange contracts.</p> <p>(d) The entry of matching buys and sells in particular securities or futures or leveraged foreign exchange contracts ("wash trading"), creating the illusion of trading. Such wash trading does not result in a bona fide market position, and might provide "cover" for a money launderer.</p> <p>(e) Wash trading through multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts. Transfers of positions between accounts that do not appear to be commonly controlled also could be a warning sign. (It should be noted that wash trading is also an indication of market manipulation and licensed corporations are expected to take appropriate steps to ensure that proper safeguards exist to prevent the firm from acting in a way which would result in the firm perpetrating any conduct which constitutes market misconduct under section 279 of the SFO).</p> <p>(f) Securities transactions occur across many jurisdictions, and in particular jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise pose higher risk.</p> <p>Settlement/custody/transfers-related</p> <p>(a) Large or unusual settlements of transactions in cash or bearer form or where a customer only deals with a licensed corporation in cash or cash equivalents.</p> <p>(b) A customer uses a licensed corporation to make payments or to hold funds and/or other property that are rarely used or are not being used to trade in securities, futures contracts or leveraged foreign exchange contracts i.e. account appears to be used as a depositary account or a conduit for transfers.</p> <p>(c) Non-resident account with very large account movements and subsequent fund transfers to offshore financial centres.</p> <p>(d) Transfers of positions, funds or other property between accounts of parties that do not appear to be commonly controlled or have an apparent relationship.</p> <p>(e) Frequent funds or other property transfers or cheque payments to or from third parties that are unrelated, unverified or difficult to verify.</p> <p>(f) Incoming payments made by cheques with multiple endorsements.</p> <p>(g) A customer allocates incoming third party deposits among numerous accounts.</p> <p>(h) The involvement of offshore companies on whose accounts multiple transfers are made, especially when they are destined for a tax haven, and to accounts in the name of companies incorporated under foreign law of which the customer may</p>
--	--	--



		<p><i>be a shareholder.</i></p> <p><i>(i) The customer's explanation regarding the method of acquiring the physical securities deposited at the licensed corporation does not make sense or changes.</i></p>
<i>ML involving employees of licensed corporations</i>		
	7.39	<p><i>(a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.</i></p> <p><i>(b) Unusual or unexpected increase in the sales performance of an employee.</i></p> <p><i>(c) The employee's supporting documentation for customers' accounts or orders is incomplete or missing.</i></p> <p><i>(d) The use of an address which is not the customer's home or office address, e.g. utilization of an employee's address for the dispatch of customer documentation or correspondence.</i></p>



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 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	<p>FIs should prepare and 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:</p> <ul style="list-style-type: none"> (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 7.31) and training records (see paragraph 9.9).

Retention of records relating to customer identity and transactions

<p>s.20(1)(b)(i), Sch. 2</p> <p>s.2(1)(c), Sch. 2</p> <p>s.20(1)(b)(ii), Sch. 2</p>	8.3	<p>FIs should keep:</p> <ul style="list-style-type: none"> (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 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 with the customer and any beneficial owner of the customer (which at a minimum should include correspondence concerning the establishment of the business relationship and ongoing 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 six years after the end of the business relationship.



s.20(1)(a), Sch. 2	8.5	<p>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. These should include the following:</p> <ul style="list-style-type: none"> (a) the identity of the parties (including beneficiary where appropriate) 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). <p>In any event, FIs should ensure the records retained are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.</p>
s. 20(2), Sch. 2	8.6	All documents and records mentioned in paragraph 8.5 should be kept for a period of six years after the completion of a transaction, regardless of whether the business relationship ends during the period.
s. 21, Sch. 2	8.7	If the record consists of a document, either the original of the document should be retained or a copy of the document should be kept on microfilm or in the database of a computer. If the record consists of data or information, such record should be kept either on microfilm or in the database of a computer.
s. 20(4), Sch. 2	8.8	An RA may, by notice in writing to an FI, require it to keep the records relating to a specified transaction or customer for a period specified by the RA that is longer than those referred to in paragraphs 8.4 and 8.6, where the records are relevant to an on-going 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. This may involve the FIs retaining a copy of the underlying records of identity and transaction in Hong Kong.



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 ³⁵ 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	<p>Staff should be made aware of:</p> <ul style="list-style-type: none"> (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	<p>In addition, the following training modules may be appropriate for certain groups of staff:</p> <ul style="list-style-type: none"> (a) all new staff, irrespective of seniority, should be given an introduction to the background to ML/TF, the need for identifying and reporting of any suspicious transactions to the MLRO, and the offence of "tipping-off". They should understand the importance placed on ML/TF issues by the FI; (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) should be made aware of the FI's policies and procedures in relation to CDD and record keeping requirements that are relevant to their job responsibilities. They are the first point of contact with potential money launderers and their efforts are vital to the FIs strategy in the fight against money laundering. They should be provided training on areas that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. They

³⁵ In the context of Chapter 9, staff include appointed insurance agents.



		<p>should know the FI's policies and procedures, including the line of reporting, for dealing with particular situations such as those where large transactions are involved, and the need for extra vigilance in these cases;</p> <p>(c) back-office staff, depending on their roles, should receive appropriate training on customer verification and relevant processing procedures as well as training on how to recognise unusual activities including abnormal settlements, payments or delivery instructions;</p> <p>(d) managerial staff including internal audit officers and COs should receive a higher level of training covering all aspects of AML/CFT procedures, in addition to 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</p> <p>(e) AML COs should have a thorough working knowledge of all relevant legislation, regulatory guidance and the FI's policies and procedures on the prevention of ML/TF. They should know the procedures for handling production and restraint orders and ensure relevant staff also possess such knowledge. They should be equipped with the knowledge and skills in assessing suspicious transaction reports submitted to them. Opportunities should be provided to enable them to keep abreast of all new developments and requirements in relation to AML/CFT.</p>
	9.8	<p>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.</p>
	9.9	<p>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.</p>
	9.10	<p>FIs should monitor the effectiveness of the training. This may be achieved by:</p> <p>(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</p> <p>(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.</p>



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 guidelines provided in this Chapter if they act as an ordering institution or beneficiary institution as defined under the AMLO. Where an FI is the originator or recipient/beneficiary of a wire transfer, it is not acting as an ordering institution or 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/beneficiary) at another 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.
s.12(2), Sch. 2	10.3	This chapter does not apply to the following wire transfers: <ul style="list-style-type: none"> (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 if each of them acts on its own behalf; (c) a wire transfer if: <ul style="list-style-type: none"> (i) it arises from a transaction that is carried out using a credit card or debit card (such as withdrawing money from a bank account through an automated teller machine with a debit card, obtaining a cash advance on a credit card, or paying for goods or services with a credit or debit card), except when the card is used to effect a transfer of money; and (ii) the credit card or debit card number is included in the message or payment form accompanying the transfer.
	10.4	For SWIFT users, the above exemption will apply to MT 200 series payments, MT 400 and MT 700 series messages when they are used to settle cheque collection and trade finance obligations between banks. Where the originator is an FI, as will sometimes be the case even for SWIFT MT 102 and MT 103 messages, supplying the Bank Identifier Code ³⁶ (BIC) of the FI constitutes complete originator information for the purposes of the AMLO, although it is also preferable for the account number to be included where available. This also applies to Business Entity Identifiers ³⁷ (BEIs), although in such case the account number should always be included. There may however be requests from beneficiary institution for address information.
	10.5	The FATF issued Special Recommendation VII (SR VII) in October 2001 ³⁸ , with the objective of enhancing the transparency of all domestic and cross-border wire transfers to make it easier for law enforcement to track funds transferred

³⁶ BIC ("Business Identifier Code") is also known as SWIFT Code.

³⁷ When BIC assigned to a non-financial organisation, e.g. a corporate, the code is called a BEI ("Business Entity Identifier").

³⁸ A revised Interpretative Note to this special recommendation was issued by the FATF on 29 February 2008 and is available on the FATF website.



		electronically by terrorists and criminals. The Basel Committee on Banking Supervision guidance paper “Due diligence and transparency regarding cover payment messages related to cross-border wire transfers” (May 2009) also describes supervisory expectations in this area.
Ordering institutions		
s.12(3), Sch. 2	10.6	<p>Ordering institutions must ensure that all wire transfers of amount equal to or exceeding HK\$8,000 (or an equivalent amount in any other currency) are accompanied by complete and verified originator information as required under section 12(3) of Schedule 2 which includes:</p> <ul style="list-style-type: none"> (a) the originator’s name; (b) the number of the originator’s account maintained with the FI and from which the money for the wire transfer is paid, or a unique reference number³⁹ (for non-account holders); and (c) the originator’s address or, in the absence of an address, the originator’s customer identification number or identification document number (e.g. HKID card number for a customer who is a natural person, or business registration number for a customer who is a legal person), or, if the originator is an individual, the originator’s date and place of birth. <p>There is also a concession for domestic wire transfers set out below (see paragraph 10.17 below).</p>
	10.7	It is acceptable for an ordering institution to include the “correspondence address” of the originator in the wire transfer message provided that the ordering institution is satisfied that the address has been verified.
s.12(4), Sch. 2	10.8	Ordering institutions must ensure that all the originator information accompanying the payment has been verified. The verification requirement is deemed to be met for account holding customers of the FI whose identity has been verified in compliance with the AMLO and this Guideline. No further verification of such account holder’s information is normally required, although ordering institutions may exercise their discretion to do so in individual cases.
s.3(c), 12(3)& (4), Sch. 2	10.9	For transactions with non-account holders, the ordering institution must verify the identity of the customer and all originator information to accompany the wire transfer involving an amount equal to or exceeding the equivalent of HK\$8,000. For an occasional wire transfer below HK\$8,000 (or the equivalent), ordering institutions are 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 exceed the equivalent of HK\$8,000. Evidence of verification must be retained with the customer information in accordance with the record keeping requirements of the AMLO (see Chapter 8).
	10.10	Ordering institutions may choose not to include all the required information in the wire transfer message accompanying a wire transfer of less than HK\$8,000 or equivalent in foreign currencies. However, the relevant information about the originator should be recorded and retained by the ordering institution and should be made available within three business days on request by the beneficiary institution or the appropriate authorities. In considering whether to apply the threshold of HK\$8,000, ordering institutions should take into account the business and

³⁹ The unique reference number assigned by the ordering institution should permit the wire transfer to be traced back to the originator.



		operational characteristics of their wire transfer activities. Ordering institutions are encouraged to include, as far as practicable, the relevant originator information in the messages accompanying all wire transfer transactions.
	10.11	For wire transfers conducted by an account holder as the originator, the originator's name and address (or permitted alternative) should correspond to the account holder. Any request to override customer information should not be entertained and any suspicion of improper motive by a customer should be reported to the ordering institution's MLRO.
	10.12	In particular, an ordering institution should exercise care if there is suspicion that a customer may be effecting a wire transfer on behalf of a third party. If a wire transfer carries the name of a third party as the ordering person or otherwise does not appear to be consistent with the usual business/activity of the customer, the customer should be asked to provide further explanation of the nature of the wire transfer.
	10.13	The relevant originator information should be recorded and retained in respect of both account holders and non-account holders.
	10.14	Ordering institutions should adopt an RBA to check whether certain wire transfers may be suspicious taking into account such factors as the name of the beneficiary, the destination and amount of the wire transfer etc.
	10.15	Ordering institutions should establish clear policies on the processing of cross-border and domestic wire transfers. The policies should address the following: <ul style="list-style-type: none"> (a) record keeping; (b) the verification of originator's identity information⁴⁰; (c) the message format and the circumstances in which the formats should be used; and (d) the information to be included in messages.
	10.16	Ordering institutions should include wire transfers in their ongoing due diligence on the business relationship with the originator and in their scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, its business and risk profile. Ordering institutions may adopt an RBA in their ongoing due diligence process. The process should be subject to regular audits to ensure its effectiveness.
Domestic wire transfers		
s.12(6), Sch. 2	10.17	Where both the ordering and beneficiary institutions are located within Hong Kong, the originator's information accompanying the wire transfer can simply be the originator's account number or a unique reference number which permits the transaction to be traced back to the originator.
s.12(6), Sch. 2	10.18	However, if requested by the beneficiary institution or the RA, complete originator information (see paragraph 10.6) must be provided by the ordering institution within 3 business days after the request is received.

⁴⁰ Where an originator is a non-account holder, institutions should follow the customer identification, verification and record keeping requirements prescribed for wire transfers in this Chapter.



Beneficiary Institutions		
	10.19	In respect of a wire transfer of any value for a beneficiary who is not an account holder, the beneficiary institution should record the identity and address of the recipient. For wire transfers equal to or exceeding HK\$8,000, the beneficiary institution should verify the recipient's identity by reference to his identity card or travel document.
Batch file transfers		
s.12(7), Sch. 2	10.20	An ordering institution may bundle a number of transfers into a batch file for transmission to an overseas beneficiary institution. In such cases, the individual transfers within the batch file need only carry the originator's customer account number (or unique reference number if there is no account number), provided that the batch file itself contains complete originator information.
Intermediary institutions		
s.12(8), Sch. 2	10.21	If an FI acts as an intermediary institution in a wire transfer, it must ensure that all originator information which accompanies the wire transfer is retained with the transfer and is passed to the next institution in the payment chain.
s.19(2), Sch. 2	10.22	The requirement to detect the lack of complete originator information applies to intermediaries in the same way as for transfers of funds received directly by the beneficiary institution.
	10.23	It is preferable for an intermediary institution to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an intermediary institution is technically unable to onward transmit originator information with transfers originating outside Hong Kong, it must advise the beneficiary institution of the originator information by another form of communication, whether within a payment or messaging system or otherwise.
Missing, incomplete or meaningless originator information		
s.19(2), Sch. 2	10.24	FIs must establish and maintain effective procedures for identifying and handling incoming wire transfers in compliance with the relevant originator information requirements.
s.12(9)(a) & s.12(10)a, Sch.2	10.25	If the domestic or cross border wire transfer is not accompanied by the originator's information, the FI must as soon as reasonably practicable, obtain the information from the institution from which it receives the transfer instruction. If the information cannot be obtained, the FI should either consider restricting or terminating its business relationship with that institution, or take reasonable measures to mitigate the ML/TF risk involved.
s.12(9)(b) & s.12(10)(b) , Sch.2	10.26	<p>If the FI is aware that the accompanying information that purports to be the originator's information is incomplete or meaningless, it must as soon as reasonably practicable take reasonable measures to mitigate the risk of ML/TF involved.</p> <p>FIs may demonstrate compliance by implementing effective risk-based procedures and systems to subject incoming payment traffic to an appropriate level of post-event random sampling to identify wire transfers that contain incomplete or meaningless originator's information. This sampling may be weighted towards transfers:</p> <p>(a) from institutions located in non-FATF member jurisdictions, particularly those that are known to have failed to adequately implement international messaging</p>



		<p>standards (i.e. SR VII);</p> <p>(b) from institutions located in high-risk jurisdictions;</p> <p>(c) that are higher value transfers; and</p> <p>(d) from institutions that are identified by such sampling as having previously failed to comply with the relevant information requirement.</p>
s.12(9)(b) & s.12(10)(b), Sch. 2	10.27	If a beneficiary institution becomes aware in the course of processing a payment that it contains meaningless or incomplete information, it must request complete originator information. Beneficiary institutions should set appropriate deadlines for the remediation of deficient transfers.
s.12(9)(b) & s.12(10)(b), Sch. 2	10.28	If the complete and meaningful information cannot be obtained by the beneficiary institution within the deadline set, it must either consider restricting or terminating its business relationship with the institution from which it receives the transfer instruction or take reasonable measures to mitigate the ML/TF risk posed, taking into account such factors as the name of the beneficiary, the origin and amount of the transfer, etc.
	10.29	Other specific measures should also be considered by the beneficiary institutions, for example, checking, at the point of payment delivery, that originator information is complete and meaningful on all transfers that are collected in cash by recipients/beneficiaries on a “pay on application and identification” basis.
	10.30	FIs should also consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion and a report to the JFIU is appropriate.
	10.31	If an ordering institution in Hong Kong regularly fails to supply the required originator information for a wire transfer involving an amount equal to or exceeding the equivalent of HK\$8,000, the beneficiary institution should report the matter to the RA. Where an ordering institution is identified as having regularly failed to comply with these information requirements, the beneficiary institution should consider taking steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that institution or deciding whether to restrict or terminate its relationship with that institution either completely or in respect of funds transfers.
	10.32	For incoming wire transfers below HK\$8,000 containing incomplete payment information (i.e. below the SRVII threshold where the requirement becomes mandatory), FIs are not precluded from requesting the complete information; however, an RBA is suggested in such circumstances.
s.20(1) Sch. 2	10.33	Records of all electronic payments and messages must be retained in accordance with the AMLO.
Cover payment messages related to cross-border wire transfers		
	10.34	The processing of cross-border wire transfers usually involves several institutions. In addition to the ordering institution and the beneficiary institution, additional institutions (cover intermediary institutions) which provide correspondent banking services to the originating institution or the beneficiary institution are often involved in the settlement of cross-border wire transfers. Cover payment messages are messages used by these institutions for the purpose of arranging funding to settle the interbank payment obligations created by cross-border wire transfers.



	10.35	For wire transfers involving cover payment messages, ordering institutions should ensure that the message they send to cover intermediary institutions contains originator and beneficiary information. The originator and beneficiary information included in the cover payment message should be identical to that contained in the corresponding direct cross-border wire transfer message sent to the beneficiary institution. Ordering institutions are encouraged, where possible, to include other identity information about the beneficiary in cover payment messages, where this is necessary to limit the risk of customer assets being incorrectly frozen, blocked or rejected, or of the cover payment being unduly delayed.
	10.36	Cover intermediary institutions should establish clear policies and procedures to ensure, in real time, that the relevant fields for storing originator and beneficiary information in cross-border cover payment messages are not blank. In addition, they should develop and implement policies and procedures to monitor if the originator and beneficiary information in the cross-border cover payment messages is manifestly meaningless or incomplete, and the monitoring may be done on a risk sensitive basis, subsequent to the processing of the transactions. Cover intermediary institutions should also implement other measures including screening the originator and beneficiary names against their database of terrorists and terrorist suspects.
	10.37	Beneficiary institutions should identify the beneficiary and verify its identity. They should also have effective risk-based procedures in place to identify and handle wire transfers lacking complete originator information.
	10.38	More detailed guidance for AIs, particularly the responsibilities of cover intermediary institutions is provided in the “Guidance Paper on Cover Payment Messages Related to Cross-border Wire Transfers” issued by the HKMA dated 8 February 2010.



APPENDIX A

Other reliable and independent sources for customer identification purposes		
s.2(1)(a)(i) v) & 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 ⁴¹ 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 to the satisfaction of an immigration officer 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.
	4	For minors born in Hong Kong who are not in possession of a valid travel document or Hong Kong identity card ⁴² , 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.

⁴¹ For avoidance of doubt international drivers permits and licences are not acceptable for this purpose.

⁴² 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.



	5	<p>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) which, in addition to confirming the company's continued registration, contains:</p> <ul style="list-style-type: none">(a) the current basic information of the company;(b) a list of the name(s) (with identification information) of current director(s) and reserve director (if any);(c) particulars of the secretary;(d) address of registered office (for local companies);(e) address of principal place of business in Hong Kong;(f) particulars of authorized representatives (for non-Hong Kong companies);(g) share capital; and(h) particulars of receiver, manager and liquidators (if any).
	6	<p>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.</p>

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: 2011-XX-XX

Money Laundering Reporting Officer,
XXXXXXX.

Fax No. : XXXX XXXX

Dear Sir/Madam,

Suspicious Transaction Report ("STR")**JFIU No.**

XX

Your Reference

XX

Date Received

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

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 :

2011-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.

XX

Your Reference

XX

Dated

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

CONFIDENTIAL 機密

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,

(XXXXXXXX)

Superintendent of Police
Head, Joint Financial Intelligence Unit

c.c. OC Case

S/N	Account holder	Account Number
1.		



GLOSSARY OF KEY TERMS AND ABBREVIATIONS

Terms / abbreviations	Meaning
AMLO	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) 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)
ICO	Insurance Companies Ordinance (Cap. 41)
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 Crime 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)



**PROPOSED PREVENTION OF MONEY LAUNDERING
AND TERRORIST FINANCING GUIDELINE
ISSUED BY THE SECURITIES AND FUTURES COMMISSION
FOR ASSOCIATED ENTITIES**



Effective Date

This Guideline will become effective on 1 April 2012 and supersedes the Prevention of Money Laundering and Terrorist Financing Guidance Note dated September 2009.



**PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING GUIDELINE
ISSUED BY THE SECURITIES AND FUTURES COMMISSION
FOR ASSOCIATED ENTITIES**

Introduction

s.399 of SFO	1	This Guideline is published under section 399 of the Securities and Futures Ordinance, Cap. 571 (SFO).
	2	Following the enactment of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO), the SFC has prepared a Guideline on Anti-Money Laundering and Counter-Terrorist Financing (the Guideline for LCs) which provides guidance to assist licensed corporations (LCs) and others to implement and comply with the AMLO and other applicable anti-money laundering (AML) / counter-terrorist financing (CFT) legislation and regulatory requirements.
	3	The purposes of the Guideline for LCs 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 LCs 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.
	4	Terms and abbreviations used in this Guideline shall be interpreted by reference to the definitions set out in the Glossary part of the Guideline for LCs. Where applicable, interpretation of other words or phrases should follow those set out in the SFO.

Associated Entities to comply with the Guideline for LCs

	5	This Guideline is intended for use by associated entities (AEs) that are not authorized financial institutions and their officers and staff.
	6	The Guideline for LCs provides a comprehensive explanation of the AML/CFT legislation in Hong Kong and practical guidance in designing and implementing policies, procedures and controls so as to meet the relevant AML/CFT statutory and regulatory requirements. AEs that are not authorised financial institutions are expected to have regard to the provisions of the Guideline for LCs as if they were themselves LCs.
	7	An AE that is an authorized financial institution should have regard to the provisions of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the Hong Kong Monetary Authority, and to paragraphs 7.38 and 7.39 of the Guideline for LCs in identifying securities, futures and leveraged foreign exchange businesses specific suspicious transactions.



	8	Given the significant differences that exist in the organisational and legal structures of different AEs, and the LCs with which they are in a controlling entity relationship, 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 this Guideline and the Guideline for LCs are neither intended to, nor should be construed as, an exhaustive list of the means of meeting the statutory and regulatory requirements.
	9	The Guideline for LCs will assist AEs to meet their AML/CFT legislative and regulatory obligations when tailored by AEs to their particular business risk profile. Departures from this Guideline, and the rationale for so doing, should be documented, and AEs will have to stand prepared to justify departures to the SFC.
s.399 of SFO	10	A failure by any person to comply with any provision of this Guideline does not by itself render the person liable to any judicial or other proceedings but, in any proceedings under the SFO before any court, this Guideline is admissible in evidence; and if any provision set out in this Guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question.
	11	Any failure by an AE to have regard to the provisions of the Guideline for LCs may reflect adversely on its fitness and properness and the fitness and properness of the intermediary of which the AE is in a controlling entity relationship.
	12	Any failure by an AE that is an authorized financial institution to have regard to the provisions of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the Hong Kong Monetary Authority or to paragraphs 7.38 and 7.39 of the Guideline for LCs may reflect adversely on its fitness and properness and the fitness and properness of the intermediary of which the AE is in a controlling entity relationship.
	13	The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.