

**ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST
FINANCING ORDINANCE (Chapter 615)**

Notice is hereby given that pursuant to section 7(1) of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Chapter 615), we hereby publish Circular No. 23-01(CR) setting out the revised Guidelines on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for the Estate Agency Sector ('the Circular') in replacement of Circular No. 18-01 (CR) under Government Notice No. 1397 in Gazette No. 9 Volume 22 published on 2 March 2018.

The Circular shall become effective on 1 June 2023 and shall supersede Circular No. 18-01 (CR).

25 May 2023

Estate Agents Authority



地產代理監管局
ESTATE AGENTS AUTHORITY

Circular

Circular No. 23-01 (CR)

Guidelines on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for the Estate Agency Sector



CONTENTS

	Page
Summary of Guidelines.....	3-8
General Introduction	9-13
Chapter 1 Money Laundering and Terrorist Financing	14-16
Chapter 2 AML/CTF Obligations	17-23
Chapter 3 Risk-based Approach and Risk Assessment.....	24-26
Chapter 4 Customer Due Diligence.....	27-49
Chapter 5 Continuous Monitoring of Business Relationship with Customers.....	50-52
Chapter 6 Reporting Suspicious Transactions	53-59
Chapter 7 Financial Sanctions, Proliferation Financing and Terrorist Financing	60-63
Chapter 8 Record-keeping.....	64-66
Chapter 9 Staff Awareness and Training	67-70
Appendix A Acronyms, terms and abbreviations.....	71-72
Appendix B Examples of specific factors in relation to ML/TF risk rating.....	73-74
Appendix C Identification and verification of customer (including beneficial owner) who is an individual.....	75-76
Appendix D Identification and verification of customer (including beneficial owner) which is a corporation.....	77-80
Appendix E Examples of situations that could give rise to suspicion...	81-82



Summary of Guidelines

Summary of the guidelines on compliance of anti-money laundering (“AML”) and counter-terrorist financing (“CTF”) requirements for the estate agency sector (with the relevant paragraph numbers in brackets):

- (A) Money laundering (“ML”)
 - What is ML (1.1-1.3)
- (B) Terrorist financing (“TF”)
 - What is TF (1.4-1.6)
- (C) AML/CTF obligations
 - Take all reasonable measures to mitigate ML/TF risks and to ensure that proper safeguards exist to prevent contravention of any requirement under Part 2 or 3 of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (“AMLO”). (2.1)
 - Develop and implement AML/CTF systems on: (2.2)
 - risk assessment;
 - customer due diligence measures;
 - continuous monitoring of customers;
 - suspicious transactions reporting;
 - record keeping; and
 - staff training.
- (D) AML/CTF systems
 - Ensure the AML/CTF systems are effective. (2.5)
 - Appoint a compliance officer (“CO”). (2.6)
 - Appoint a money laundering reporting officer (“MLRO”). (2.7)
 - Review the implementation of the AML/CTF controls through the compliance and audit function. (2.11)
 - Screen staff to ensure good conduct and integrity and provide appropriate training to staff. (2.13-2.14)
- (E) Risk-based Approach (“RBA”)
 - Adopt an RBA in taking measures to manage and mitigate



ML/TF risks which are proportionate to the risks identified.
(3.1)

(F) Risk Assessment

- Identify, assess and understand ML/TF risks. (3.5)
- Assess the ML/TF risks by assigning a ML/TF risk rating to a customer. (3.9)
- Consider the following risk factors: (3.9)
 - customer risk;
 - country/geographic risk;
 - service risk;
 - delivery channel risk; and
 - the more specific factors are at Appendix B.
- Keep records and relevant documents of the risk assessment. (3.11)

(G) Apply the customer due diligence (“CDD”) requirements. (4.3)

- Identify the customer.
- Verify the customer’s identity.
- Where there is a beneficial owner in relation to the customer:
 - identify the beneficial owner’s identity; and
 - take reasonable measures to verify the beneficial owner’s identity.
- If a person purports to act on behalf of the customer: (4.19)
 - identify that person;
 - take reasonable measures to verify that person’s identity; and
 - verify that person’s authority to act on behalf of the customer.

(H) Timing (4.11-4.12)

- Complete the CDD process before establishing any business relationship or carrying out a specified occasional transaction.
- May complete the CDD process after establishing the business relationship, if:
 - any ML/TF risk is effectively managed; and
 - this is necessary not to interrupt the normal conduct of



business.

- A licensee that carries out verification after establishing a business relationship with a customer must complete the verification as soon as reasonably practicable. (4.13)
 - Adopt appropriate risk management policies and procedures where a business relationship is established prior to identity verification. (4.14)
- (I) When a licensee is unable to complete the CDD process, he: (4.15)
- must not establish a business relationship or carry out any occasional transaction;
 - must terminate the established business relationship as soon as reasonably practicable; and
 - should consider filing a suspicious transaction report (“STR”) with the Joint Financial Intelligence Unit (“JFIU”).
- (J) Identify and verify customer’s identity (4.16-4.17)
- Identify and verify the customer’s identity by reference to documents, data or information provided by a reliable and independent source.
 - Follow the guidance for the identification and verification of customers and their beneficial owners at Appendices C and D.
- (K) Identify and verify customer’s beneficial owner (4.18)
- Take reasonable measures to verify the identity of a beneficial owner so as to know who the beneficial owner is and to understand the ownership and control structure of the customer if it is a legal person.
 - A beneficial owner in relation to a corporation is an individual who owns or controls, directly or indirectly, more than 25% of the issued share capital or voting rights, or who exercises ultimate control over the management of the corporation.
 - For companies with multiple layers in their ownership structures (4.18(g))
 - obtain a director’s declaration annexing an ownership chart so as to identify the names and place of incorporation of all

the companies in the intermediate layers and to identify the individuals, who are the beneficial owners of the customer; and

- verify the identity of those individuals, who are the beneficial owners of the customer.

(L) Simplified CDD (“SCDD”) (4.20-4.22)

- Identify the customer.
- Verify the customer.
- There is no need to identify the beneficial owner or to verify his identity.
- Customers to whom SCDD may be applied are set out in Section 4(3) of Schedule 2 to the AMLO. (4.22)

(M) Enhanced CDD (“ECDD”)

- Take additional measures in high-risk situations e.g.:
 - customer not physically present for identification purposes; (4.27-4.29)
 - customer or his beneficial owner being a Hong Kong or Non-Hong Kong politically exposed person (“PEP”); (4.30-4.39)
 - customer from high-risk jurisdiction; (4.40)
 - any situation that by its nature may present a higher risk of ML/TF; (4.26) and
 - any situation specified in a notice given by the EAA. (4.42)
- Except as otherwise specified, if a customer or beneficial owner is a PEP, apply the following measures: (4.35)
 - obtain approval from the senior management;
 - take reasonable measures to establish the customer’s or beneficial owner’s source of wealth and the source of the funds involved in the business relationship; and
 - apply enhanced monitoring.

(N) Pre-existing customers

- Perform CDD measures in respect of pre-existing customers in certain situations. (4.46)



- (O) Continuous monitoring (5.2)
- Review from time to time information of the customer to ensure it is up-to-date and relevant.
 - Conduct scrutiny of transactions to ensure that they are consistent with the customer's business, risk profile and source of funds.
 - Identify complex transactions that have no apparent economic or lawful purpose.
- (P) Reporting suspicious transactions
- Make a STR to the JFIU once a transaction is identified or suspected to be related to ML/TF activity. (6.1)
 - Failing to report knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. (6.4)
 - MLRO should act as a central reference point for reporting suspicious transactions to the JFIU. (6.13)
 - Establish and maintain a record of all STRs made to the JFIU. (6.25)
- (Q) Financial Sanctions, Proliferation Financing and Terrorist Financing
- Conduct name checks of customers and beneficial owners against the latest lists of the designated individuals and entities that are subject to financial sanctions and of terrorist suspects. (7.6, 7.15)
 - Have an appropriate system to conduct name checks against the relevant up-to-date lists of names of the designations and terrorist suspects. (7.7, 7.16)
- (R) Record-keeping
- In respect of each customer, (8.3)
 - keep the original or a copy of the documents, and a record of the data and information for identifying and verifying the identity of the customer or any beneficial owner of the customer in accordance with Part 2 of Schedule 2 to the AMLO;

- keep the original or a copy of the files relating to the customer's business relationship and business correspondence with the customer and any beneficial owner of the customer;
 - keep the relevant records throughout the continuance of the business relationship with the customer and for a period of at least **five** years beginning on the date on which the business relationship ends; and
 - for an occasional transaction, keep the relevant records for a period of at least **five** years beginning on the date on which the occasional transaction is completed.
- In respect of each transaction, (8.4)
- keep the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction in accordance with Part 2 of Schedule 2 to the AMLO; and
 - keep the relevant records for a period of at least **five** years beginning on the date on which the transaction is completed.

(S) Staff awareness and training

- Conduct awareness and training programmes on the effective implementation of AML/CTF systems for: (9.4)
 - new staff
 - front-line staff
 - back-office staff
 - managerial staff
 - MLRO
- Monitor the effectiveness of the training. (9.6)

General Introduction

FATF

The Financial Action Task Force (“FATF”) is an inter-governmental body established in 1989 that sets international standards on combating money laundering (“ML”) and terrorist financing (“TF”). Over the years, the FATF has published a set of recommendations (“FATF Recommendations”) on anti-money laundering (“AML”) and counter-terrorist financing (“CTF”) measures. One of the FATF Recommendations is that customer due diligence (“CDD”) and record-keeping requirements apply to financial institutions as well as designated non-financial businesses and professions (“DNFBPs”), which include real estate agents, when DNFBPs engage in specified transactions. As a member of the FATF, Hong Kong is obliged to implement a credible AML/CTF regime, having regard to the FATF Recommendations.

AMLO

In April 2012, the Legislative Council enacted the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) to prescribe statutory CDD and record-keeping requirements for financial institutions in accordance with the FATF Recommendations. In January 2018, the Legislative Council enacted the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance 2018 (“2018 Amendment Ordinance”), which extends the statutory CDD and record-keeping requirements under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (“AMLO”) to cover DNFBPs, which include estate agents¹, when they engage in specified transactions. In December 2022, the Legislative Council enacted the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance

¹ “Estate agent” in the AMLO means (a) a licensed estate agent; or (b) a licensed salesperson, both as defined by section 2(1) of the Estate Agents Ordinance.

2022 to, amongst others, make miscellaneous amendments relevant to the estate agency sector.

Amendment to EAO

Subsequent to the passing of the 2018 Amendment Ordinance, consequential amendments were made to the Estate Agents Ordinance (Cap. 511) (“EAO”) to the effect that non-compliance with the AML/CTF requirements under the AMLO may trigger the application of the following provisions in the EAO: suspension or revocation of licence under section 27, investigation under section 28 and the provisions on disciplinary actions under section 29.

Guidelines

The Guidelines on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for the Estate Agency Sector (“Guidelines”) set out in this Circular are issued under section 7 of the AMLO by the Estate Agents Authority (“the EAA”), the regulatory body² for the licensees³, to provide guidance for licensees when they are involved, in Hong Kong, in a transaction concerning the buying or selling of real estate for a client⁴.

In so far as ML/TF risks in property transactions are concerned, the role played by licensees in property transactions in Hong Kong is rather limited. Their main function is that of a “middleman” between potential buyers and sellers in arranging property inspections and the signing of provisional agreements for sale and purchase (“PASP”). Unlike estate agents in other jurisdictions, licensees in Hong Kong do not act as escrow agents for receiving deposits or proceeds on behalf of clients. The amount of the initial deposit usually paid on the signing of a PASP is normally only 3% to 5% of the purchase price and is often paid by

² Section 1 in Part 2 of Schedule 1 to the AMLO refers.

³ Licensee(s) means holder(s) of an Estate Agent’s Licence (Individual), Estate Agent’s Licence (Company) or a Salesperson’s Licence (as the case may be) granted under the EAO.

⁴ Section 5A(4) of the AMLO refers.

way of a personal cheque from the buyer directly to the seller or the seller's solicitors as stakeholders. Therefore, it is rare for licensees to receive the purchase money for clients and so the risk of ML/TF in the estate agency sector should be relatively low.

Given that a PASP is usually superseded by a subsequent formal agreement for sale and purchase or an assignment which will be handled by legal professionals, another DNFBP covered under the AMLO, and that banks are often involved in the process of fund transfer in property transactions, clients would invariably be subject to the same set of AML/CTF measures imposed by legal professionals and financial institutions under the AMLO. Against this background, the EAA has adopted a risk-based approach as advocated by the FATF for combating ML/TF in formulating the Guidelines, proportionate to the ML/TF risks faced by the estate agency sector.

Purpose of Guidelines

The purposes of the Guidelines are to provide:

- (a) a general background on the subjects of ML and TF; and
- (b) practical guidance to assist licensees and their senior management⁵ in devising and implementing policies, procedures and controls in relevant operational areas, taking into consideration their own circumstances so as to meet the relevant AML and CTF requirements under Schedule 2 to the AMLO.

Objectives of Guidelines

After studying the Guidelines, licensees should be able to:

- (a) understand their responsibilities in respect of AML and CTF;
- (b) appreciate the risks of ML and TF specific to the estate agency sector;
- (c) identify suspicious transactions in the course of their practice; and

⁵ The meaning of "senior management" is set out in **Appendix A**.

- (d) understand their legal obligations to report suspicious transactions.

Guidelines not exhaustive

Given the differences that exist in the organisational and legal structures of different estate agency companies⁶ as well as the scope of their business activities, the Guidelines are neither intended to be, nor should they be construed as, the only means of meeting the statutory requirements.

Guidelines not legal advice

While the Guidelines are intended to explain and supplement the relevant statutory requirements, they do not constitute legal advice. Licensees are advised to seek independent legal advice as they see fit.

Failure to observe Guidelines

A failure by a licensee to comply with any provision in the Guidelines does not by itself render the licensee liable to any judicial or other proceedings, but in any proceedings under the AMLO before any court, the Guidelines are admissible in evidence; and if any provision set out in the Guidelines appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question⁷. Similarly, in considering whether a licensee has contravened a relevant provision in the EAO concerning an AML/CTF requirement as therein defined, the EAA will have regard to the relevant provision in the Guidelines. Subject to the aforesaid and for the avoidance of doubt, the EAA may take disciplinary actions against a licensee for any contravention of the relevant provisions in the EAO concerning an AML/CTF requirement as therein defined, and/or failure to comply with any provision in the Guidelines.

⁶ The term “estate agency company” refers to a business entity (whether a company, partnership or sole proprietorship) which is a licensed estate agent under the EAO.

⁷ Section 7(4) of the AMLO refers.

Terms and words used, etc.

The acronyms, terms and abbreviations used in the Guidelines are at **Appendix A**.

In the Guidelines, the words “must” and “is/are required” denote a legal or regulatory obligation. The word “should” denotes a recommendation of good practice, which is also a standard that licensees are expected to follow. A licensee is also expected to be able to explain the reasons for any departure from that standard.

Words importing a gender include every gender. No gender preference is intended.

Effective date

This Circular No. 23-01(CR) supersedes Circular No. 18-01(CR) and shall take effect on 1 June 2023.

May 2023

Holders of Statements of Particulars of Business
 must bring this Circular to the attention of all staff
 engaged in estate agency work



Chapter 1

MONEY LAUNDERING AND TERRORIST FINANCING

Money Laundering

- 1.1 In simple terms, money laundering (“ML”) is how criminals change crime proceeds (including money and other assets) into clean money or assets that have no obvious link to their criminal origins.

- 1.2 ML can take many forms, but in the property sector, it may involve:
 - (a) buying a property asset using the proceeds of crime and selling it on, giving the criminal an apparently legitimate source of funds;
 - (b) criminals hiding behind complex company structures and multiple bank accounts to disguise the real purpose of a transaction and to hide its beneficial ownership; and
 - (c) paying an estate agency company an exceptionally big deposit and reclaiming it later.

- 1.3 The term “money laundering” is defined in section 1 of Part 1 of Schedule 1 to the AMLO as an act intended to have the effect of making any property:
 - (a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or
 - (b) that in whole or in part, directly or indirectly, represents such proceeds,
not to appear to be or so represent such proceeds.



Terrorist Financing

- 1.4 Terrorists require funds to carry out acts of terrorism and terrorist financing (“TF”) provides the funds needed. TF involves dealing with money or property that one knows or has reasonable cause to suspect may be used for terrorism. The funds and property may be from legitimate sources or criminal sources. They may be in small amounts.
- 1.5 There is often a need for terrorists to obscure or disguise links between them and their funding sources. 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.
- 1.6 The term “terrorist financing” is defined in section 1 of Part 1 of Schedule 1 to the AMLO as:
- (a) the provision or collection, by any means, directly or indirectly, of any property –
 - (i) with the intention that the property be used; or
 - (ii) knowing that the property will be used,in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);
 - (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or
 - (c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

Criminal offences

- 1.7 Both ML and TF are criminal offences under the laws of Hong Kong. Under the Drug Trafficking (Recovery of Proceeds)

Ordinance (Cap. 405) (“DTROPO”) and the Organized and Serious Crimes Ordinance (Cap. 455) (“OSCO”), a person commits the offence of ML if he deals with any property, including money, which he knows or has reasonable grounds to believe to be proceeds of drug trafficking or an indictable offence. Under the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) (“UNATMO”), a person commits the offence of TF if he provides or collects any property knowing or with the intention that such property will be used to commit a terrorist act.

Chapter 2 AML/CTF OBLIGATIONS

General obligations

- 2.1 According to section 23 of Schedule 2 to the AMLO, licensees are required to take all reasonable measures to:
- (a) mitigate the risk of ML/TF; and
 - (b) ensure that proper safeguards exist to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2 to the AMLO.
- 2.2 To fulfil the above-mentioned obligations, estate agency companies and senior management should assess the ML/TF risk of their practices or businesses, develop and implement policies, procedures and controls (“AML/CTF systems”):
- (a) risk assessment;
 - (b) CDD measures;
 - (c) continuous monitoring of customers;
 - (d) suspicious transactions reporting;
 - (e) record keeping; and
 - (f) staff training.

AML/CTF systems

- 2.3 Estate agency companies and senior management should establish and implement adequate and appropriate AML/CTF systems (including customer acceptance policies and procedures) taking into account factors including services offered, types of customers and geographical locations involved.
- 2.4 For the proper implementation of policies and procedures, there should be:
- (a) senior management oversight;
 - (b) appointment of compliance officer (“CO”) and money laundering reporting officer (“MLRO”);

- (c) compliance and audit function; and
- (d) staff screening and training.

Senior management oversight

2.5 Senior management should:

- (a) ensure that their AML/CTF systems are capable of mitigating the ML/TF risks identified;
- (b) appoint a director or senior manager as the CO who has overall responsibility for the establishment and maintenance of their AML/CTF systems; and
- (c) appoint a senior member of their staff as the MLRO who is the central reference point for reporting suspicious transactions.

Compliance Officer

2.6 The major responsibilities of the CO are as follows:

- (a) to be responsible for the estate agency company's compliance with the AML/CTF requirements;
- (b) to act as the focal point within the estate agency company for the oversight of all activities relating to the prevention and detection of ML/TF;
- (c) to provide support and guidance to the senior management to ensure that ML/TF risks are adequately managed;
- (d) to develop and/or continuously review the estate agency company's AML/CTF systems to ensure they remain up-to-date and meet current statutory and regulatory requirements;
- (e) to oversee all aspects of the estate agency company's AML/CTF systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
- (f) to carry out regular audits on compliance with the AML/CTF requirements; and
- (g) to oversee relevant staff screening to ensure that they have

the ability to carry out their functions and are of good conduct and integrity.

Money Laundering Reporting Officer

2.7 The major responsibilities of the MLRO are as follows:

- (a) to review all internal reports of suspicious transactions and exception reports and, in the light of all available information, determine whether or not it is necessary to file a suspicious transaction report (“STR”) with the Joint Financial Intelligence Unit (“JFIU”);
- (b) to maintain all records relating to such internal reviews;
- (c) to provide guidance to staff on how to avoid “tipping off” if any STR is filed; and
- (d) to act as the main point of contact with the JFIU, law enforcement agencies, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

2.8 In order that the CO and MLRO may discharge their responsibilities effectively, estate agency companies and senior management should, as far as practicable, ensure that the CO and MLRO are:

- (a) independent of all operational and business functions, subject to the constraint of the size of the licensee’s business;
- (b) based in Hong Kong;
- (c) of a sufficient level of seniority and authority within the estate agency company;
- (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 ML/TF risks;

- (e) fully conversant with the AML/CTF statutory and regulatory requirements for a licensee and the ML/TF risks arising from the estate agency company's business;
- (f) capable of accessing, on a timely basis, all available information, both from internal sources (such as CDD records) and external sources (such as circulars issued by the EAA); and
- (g) equipped with sufficient resources, including staff and appropriate cover for the absence of the CO and MLRO (for example, an alternate or deputy CO and MLRO).

2.9 Depending on the operation and risk profile of an estate agency company, the same person may be appointed as its CO and MLRO.

2.10 In order to effectively discharge those responsibilities, the CO should have regard to the different aspects of the estate agency company's AML/CTF systems, including:

- (a) the means by which the AML/CTF systems are managed and tested;
- (b) the identification and rectification of deficiencies in the AML/CTF systems;
- (c) the number of internal reports of suspicious transactions and STRs filed with the JFIU;
- (d) the mitigation of ML/TF risks arising from business relationships and transactions with persons (including both natural and legal persons) from countries which do not or insufficiently adopt the recommendations of the FATF;
- (e) the communication with senior management of key AML/CTF issues including, where appropriate, significant compliance deficiencies;
- (f) changes made or proposed in respect of new legislation, regulatory requirements or guidelines;
- (g) compliance with any requirement under Part 2 or 3 of

Schedule 2 to the AMLO by branches and subsidiary undertakings outside Hong Kong; and

- (h) AML/CTF training for staff.

Compliance and audit function

- 2.11 The compliance and audit function should review the implementation of the AML/CTF controls, e.g. by sample testing (in particular, the controls for recognising 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 estate agency company's business.
- 2.12 Where practicable, estate agency companies and senior management should establish an independent compliance and audit function which should have a direct line of communication to the senior management.

Staff screening and training

- 2.13 Estate agency companies and senior management should establish, maintain and operate appropriate procedures to screen relevant staff before they take up their post to assess that they are effective in carrying out their function and are of good conduct and integrity.
- 2.14 Estate agency companies and senior management should provide appropriate training⁸ to staff in AML/CTF matters.

Duties extended to branches and subsidiary undertakings outside Hong Kong⁹

- 2.15 An estate agency company which is incorporated in Hong Kong but has branches or subsidiary undertakings outside Hong Kong must ensure that its branches and subsidiary undertakings that carry on the same business as the estate agency company in a

⁸ For further guidance on staff training, see Chapter 9.

⁹ Section 22 of Schedule 2 to the AMLO refers.

place outside Hong Kong have procedures in place to ensure compliance with, to the extent permitted by the law of that place, the CDD and record-keeping requirements similar to those imposed under Parts 2 and 3 of Schedule 2 to the AMLO. The estate agency company should have in place a group AML/CTF policy and communicate the group policy to its branches and subsidiary undertakings outside Hong Kong.

- 2.16 If a branch or subsidiary undertaking of an estate agency company outside Hong Kong is unable to comply with the requirements that are similar to those imposed under Parts 2 and 3 of Schedule 2 to the AMLO because this is not permitted by the law of the place at which the branch or subsidiary undertaking carries on business, the estate agency company must:
- (a) inform the EAA of such failure; and
 - (b) take additional measures to effectively mitigate the ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.
- 2.17 To the extent permitted by the laws and regulations of the jurisdictions involved and subject to adequate safeguards on the protection of confidentiality and use of information being shared, including safeguards to prevent tipping-off, an estate agency company incorporated in Hong Kong, which has branches or subsidiary undertakings outside Hong Kong, should also implement measures, through its group-wide AML/CTF systems, for:
- (a) sharing information required for the purposes of CDD and ML/TF risk management; and
 - (b) provision to the estate agency company's group-level compliance, audit and/or AML/CTF functions, of customer, account, and transaction information from its branches and subsidiary undertakings outside Hong Kong that carry on the same business as an estate agent as defined in the AMLO,

when necessary for AML/CTF purposes¹⁰.

Co-operate with EAA

- 2.18 Licensees are required to co-operate with the EAA in pursuit of its duties and must forthwith, upon the EAA's request, provide it with the risk assessment information and the records and documents in relation to their compliance with the AML/CTF requirements.

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



Chapter 3

RISK-BASED APPROACH AND RISK ASSESSMENT

Risk-based Approach

- 3.1 A risk-based approach (“RBA”) is where an estate agency company and senior management assess the risks that their practice or business may be used for ML/TF, and put in place appropriate measures to manage and mitigate those risks. An RBA should balance the costs to the estate agency company’s business and customers with a realistic assessment of the risk that criminals may exploit the business for ML/TF. It allows the estate agency company and senior management to focus its efforts on the most important areas and reduce unnecessary burdens.
- 3.2 An RBA helps ensure that measures to prevent ML/TF activities are proportionate to the risks identified and to facilitate decisions on how to allocate resources in the most effective way. The general principle of an RBA is that where customers are assessed to be of higher ML/TF risks, licensees should take enhanced measures to manage and mitigate those risks, and where the risks are lower, simplified measures may be applied.
- 3.3 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 risk receives the highest attention.
- 3.4 While there are no universally accepted methodologies that prescribe the nature and extent of an RBA, an effective RBA involves identifying and categorising ML/TF overall risks at the customer level and establishing reasonable measures based on the risks identified. An effective RBA will allow licensees to exercise reasonable business judgment with respect to their customers.



Risk Assessment

- 3.5 Licensees should take appropriate steps to identify, assess and understand their ML/TF risks and take effective action to mitigate them.
- 3.6 Licensees should identify and assess the ML/TF risks that may arise in relation to:
 - (a) the development of new services and new business practices; and
 - (b) the use of new or developing technologies for both new and pre-existing services.
- 3.7 Licensees should conduct the risk assessment prior to the launch of the new services, new business practices, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.
- 3.8 In assessing ML/TF risks, licensees should consider all the relevant risk factors before determining what the level of overall risk is and the appropriate level and type of mitigation to be applied and document their risk assessment.
- 3.9 Licensees may assess the ML/TF risks of individual customers by assigning a ML/TF risk rating to their customers. While there is neither an agreed set of risk factors nor a single methodology to apply these risk factors in determining the ML/TF risk rating of customers, the following factors may be considered:
 - (a) customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of politically exposed person (“PEP”), types of occupation, etc.);

- (b) country/geographic risk¹¹ (e.g. customers with residence in or connection with high-risk jurisdictions e.g. countries identified by the FATF as having deficient systems to prevent ML/TF, etc.);
- (c) service risk (e.g. services that inherently have provided more anonymity, large cash payments, payments received from unassociated or unknown third parties, etc.); and
- (d) delivery channel risk (e.g. on-line or other non face-to-face, cross boundary service etc.).

3.10 Some examples of the more specific factors in relation to the assessment of the ML/TF risk rating of customers are at **Appendix B**.

Documenting risk assessment

3.11 Licensees should keep records and relevant documents of the risk assessment, which are capable of being reproduced in a legible form.

¹¹ In assessing country risk associated with a customer, consideration may be given to local legislation (such as the United Nations Sanctions Ordinance, Cap. 537 (“UNSO”) and the UNATMO), data available from the United Nations, the International Monetary Fund, the World Bank, the FATE, etc. and the licensee’s own experience which may have indicated weaknesses in other jurisdictions.

Chapter 4 CUSTOMER DUE DILIGENCE (“CDD”)

- 4.1 CDD is intended to enable a licensee to form a reasonable belief that he knows the true identity of the customer concerned and, with an appropriate degree of confidence, knows the type of business and transactions the customer is likely to undertake. By carrying out CDD on customers, licensees may use the CDD information as an important tool to recognise whether there are grounds for suspicion of ML/TF activities.
- 4.2 The CDD requirements are set out in Schedule 2 to the AMLO. Depending on specific circumstances, licensees may also need to conduct additional measures (referred to as enhanced customer due diligence (“ECDD”) hereinafter) or, alternatively, simplified customer due diligence (“SCDD”).

APPLYING CDD

Customary CDD Measures

- 4.3 The CDD measures applicable to licensees under section 2 of Schedule 2 to the AMLO are:
- (a) **identifying the customer and verifying the customer’s identity** using documents, data or information from reliable and independent source;
 - (b) where there is a beneficial owner in relation to the customer, **identifying the beneficial owner and taking reasonable measures to verify the beneficial owner’s identity** so that the licensee is satisfied that he knows who the beneficial owner is, including in the case where the customer is a legal person or trust, measures to enable the licensee to understand the ownership and control structure of the legal person or trust;

- (c) obtaining information on the purpose and intended nature of the business relationship (if any) established with the licensee although in most cases, this will be self-evident for estate agency businesses; and
- (d) if a person purports to act on behalf of the customer:
 - (i) identifying the person and taking reasonable measures to verify the person’s identity using documents, data or information from reliable and independent source; and
 - (ii) verifying the person’s authority to act on behalf of the customer.

4.4 Under section 1 in Part 2 of Schedule 1 to the AMLO, a “customer” is defined to include a client. While the meaning of “customer” and “client” should be inferred from its everyday meaning and in the context of industry practice, it should be noted that the term “client” in section 5A(4) of the AMLO is as defined by section 2(1) of the EAO, which means *“any person who whether on his own behalf or on behalf of another person retains or otherwise uses the services of, or otherwise engages or employs, an estate agent”*.

4.5 In the context of the estate agency sector, a customer, often referred to as a client, can be a seller (who is often the owner(s) of the property) or a buyer of the property.

4.6 Pursuant to section 3(1) of Schedule 2 to the AMLO, licensees **must** carry out CDD:

- (a) before establishing a business relationship¹² with the customer;
- (b) before carrying out for the customer an occasional

¹² For the avoidance of doubt and for the purposes of the AMLO, a property viewing arranged by a licensee and attended by a prospective purchaser does not constitute a business relationship. In other words, CDD is only applicable when the sale and purchase of a property takes place.



transaction that involves an amount equal to or above \$120,000¹³ or an equivalent amount in any other currency, whether the transaction is carried out in a single operation or in several operations that appear to the licensee to be linked;

- (c) when the licensee suspects that the customer or the customer's account is involved in ML/TF;
- (d) when the licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity.

4.7 Under section 1 of Schedule 2 to the AMLO,

- (a) "business relationship" is defined to mean a business, professional or commercial relationship between a licensee and a person that has an element of duration, or at the time when the person first contacts the licensee in the person's capacity as a potential customer, the licensee expects the relationship to have an element of duration; and
- (b) "occasional transaction" is defined to mean a transaction between a licensee and a customer who does not have a business relationship with the licensee.

4.8 In most cases, a sale and purchase of a property involves an element of duration and so a business relationship is formed between a licensee and his customer.

4.9 In the case of dual agency, since a licensee enters into a business relationship with both parties to a transaction i.e. the property seller and the property buyer, both the seller and the buyer are the licensee's clients (i.e. customers) and the CDD requirements are therefore required to be applied to both parties to the transaction.

¹³ The value of the transaction here means the gross value of the property transaction, not the value of the deposit payable under the property transaction or the licensee's commission.

- 4.10 In the case of single agency and if a licensee acts for one party only but not the other party, the party for whom the licensee acts is the licensee's client (i.e. customer) and thus the CDD requirements are required to be applied to that party only.

Timing¹⁴

- 4.11 A licensee must complete the CDD process **before** establishing any business relationship or before carrying out a specified occasional transaction.
- 4.12 However, licensees may verify the identity of the customer and any beneficial owner **after** establishing the business relationship, if:
- (a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity is effectively managed; and
 - (b) this is necessary not to interrupt the normal conduct of business with regard to the customer.
- 4.13 A licensee that carries out verification after establishing a business relationship with a customer must complete the verification as soon as reasonably practicable after establishing the business relationship.

Failure to complete CDD

- 4.14 Where a customer is permitted to utilize the business relationship prior to identity verification, licensees should adopt appropriate risk management policies and procedures which may include:
- (a) establishing timeframes for the completion of the identity verification measures;
 - (b) regular monitoring of such relationships pending completion

¹⁴ Section 3 of Schedule 2 to the AMLO refers.

of the identity verification, and keeping senior management informed of any pending completion cases;

- (c) obtaining all other necessary CDD information;
- (d) ensuring verification of identity is carried out as soon as it is reasonably practicable;
- (e) informing the customer of the licensee'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 and type of transactions that can be undertaken pending verification; and
- (g) ensuring that funds are not paid out to any third party, though exceptions may be made to allow payments to third parties under the following conditions:
 - (i) there is no suspicion of ML/TF;
 - (ii) the risk of ML/TF is assessed to be low;
 - (iii) the transaction is approved by senior management, who should have taken into consideration the nature of the business of the customer before approving the transaction;
 - (iv) the names of the recipients do not match with those on the watch lists such as those for terrorist suspects and PEPs; and
 - (v) reasonable measures have been taken to effectively manage any ML/TF risk involved.

4.15 Where a licensee is unable to complete the CDD process, he:

- (a) must not establish a business relationship or carry out any occasional transaction with that customer;
- (b) must terminate the business relationship as soon as reasonably practicable if he has already established a business relationship with that customer; and
- (c) should assess whether failure to complete the CDD process provides grounds for knowledge or suspicion of ML/TF and

for filing a STR with the JFIU.

Identifying and verifying customer's identity¹⁵

4.16 Licensees must identify the customer and verify the customer's identity by reference to documents, data or information provided by:

- (a) a governmental body;
- (b) the EAA;
- (c) an authority in a place outside Hong Kong that performs functions similar to those of the EAA;
- (d) a recognised digital identification system¹⁶; or
- (e) any other reliable and independent source that is recognised by the EAA.

4.17 Guidance for the identification and verification of a customer who/which is an individual or a corporation (including their beneficial owners) is set out in **Appendices C and D** to the Guidelines.

4.18 Identifying and verifying customer's beneficial owner¹⁷

- (a) A beneficial owner refers to an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted.
- (b) In respect of a customer who is an individual not acting in an official capacity on behalf of a legal person or trust, the customer himself is normally the beneficial owner but the licensee should make appropriate enquiries where there are indications that the customer is not acting on his own behalf. For example, a father who provides the fund for the purchase and controls the purchaser customer who is his son

¹⁵ Section 2(1)(ab) of Schedule 2 to the AMLO refers.

¹⁶ A digital identification system that is a reliable and independent source that is recognised by the EAA.

¹⁷ Section 1(1) and Section 2(1)(b) of Schedule 2 to the AMLO refer.



and a student.

- (c) A beneficial owner in relation to a corporation is an individual who owns or controls, directly or indirectly, more than 25% of the issued share capital or voting rights, or who exercises ultimate control over the management of the corporation, or if the corporation is acting on behalf of another person, means the other person.
- (d) A beneficial owner in relation to a partnership is an individual who is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or who exercises ultimate control over the management of the partnership; or if the partnership is acting on behalf of another person, means the other person.
- (e) A beneficial owner in relation to a trust is a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not; or the settlor of the trust; or the trustee of the trust; or a protector or enforcer of the trust; or an individual who has ultimate control over the trust.
- (f) The obligation to verify the identity of a beneficial owner is for the licensee to take **reasonable measures**, based on his assessment of the ML/TF risk, so that he is satisfied that he knows who the beneficial owner is, including measures to enable him to understand the ownership and control structure of the customer if it is a legal person or trust.
- (g) For companies with multiple layers in their ownership structures, the intermediate layers of the companies should all be identified. The manner in which this information is collected should be determined by the licensee by, for example, obtaining a director's declaration annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk

sensitive basis but should at least include the company name and place of incorporation). The objective should always be to follow the chain of ownership to the individuals who are the beneficial owners of the direct customer of the licensee and verify the identity of those individuals.

- (h) Where the ownership is dispersed, the licensee 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) For the guidance on the identification and verification of the beneficial owner of a customer who/which is an individual or a corporation, please refer to **Appendices C and D**.

4.19 **Identifying and verifying a person purporting to act on behalf of a customer**¹⁸

- A. If a person purports to act on behalf of a customer (herein referred to as a “representative”), licensees must:
 - (a) identify the representative and take **reasonable measures** to verify the representative’s identity on the basis of documents, data or information provided by-
 - (i) a governmental body;
 - (ii) the EAA;
 - (iii) an authority in a place outside Hong Kong that performs functions similar to those of the EAA; or
 - (iv) any other reliable and independent source that is recognised by the EAA; and
 - (b) verify the representative’s authority to act on behalf of the customer.
- B. The general requirement is to obtain the identification information as set out in paragraph 1 of **Appendix C** from

¹⁸ Section 2(1)(d) of Schedule 2 to the AMLO refers.

the representative. In taking measures to verify the identity of the representative (e.g. authorised signatories and attorneys), a licensee should refer to the documents and other means listed in **Appendix C** wherever possible. As a general rule, licensees should identify and verify the identity of those authorised to give them instructions for the movement of funds or assets.

- C. Licensees must obtain written authority (such as power of attorney, board resolution or similar written authority for corporations) to verify that the representative is authorised to represent the customer.

APPLYING SCDD

Application of SCDD¹⁹

4.20 The AMLO defines what CDD measures are and also prescribes the circumstances in which a licensee must carry out CDD. SCDD means that application of customary CDD measures is not required. In practice, this means that where SCDD applies (see paragraph 4.22 below), the licensee is not required to identify the beneficial owner or to verify his identity.

4.21 Nonetheless, SCDD must not be applied when the licensee suspects that the customer, the customer's account or the transaction is involved in ML/TF, or when the licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or verifying the customer's identity, notwithstanding that the type of customers falls within paragraph 4.22 below (see section 3(1)(d) and (e) of Schedule 2 to the AMLO).

To whom may SCDD be applied?

4.22 Pursuant to section 4(3) of Schedule 2 to the AMLO, customers to

¹⁹ Section 4 of Schedule 2 to the AMLO refers.

whom SCDD may be applied are:

- (a) a financial institution;
- (b) an institution that-
 - (i) is incorporated or established in an equivalent jurisdiction²⁰;
 - (ii) carries on a business similar to that carried on by a financial institution;
 - (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
 - (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities²¹;
- (c) a corporation listed on any stock exchange;
- (d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is-
 - (i) a financial institution;
 - (ii) an institution incorporated or established in Hong Kong, or 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;
- (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

²⁰ “Equivalent jurisdiction” referred to in the Guidelines means a jurisdiction which is a member of FATF or which imposes requirements similar to those imposed under Schedule 2 to the AMLO.

²¹ “Relevant authority”, as defined in section 1 of Part 2 of Schedule 1 to the AMLO, include the Monetary Authority, Securities and Future Commission, Insurance Authority, Commissioner of Customs and Excise and Registrar of Companies.

those of a public body.

4.23 To ascertain whether a customer is within categories (a) to (d) of paragraph 4.22, it will be generally sufficient for licensees to:

- (a) verify that the customer is a financial institution or institution on the list of authorised (or supervised) financial institutions in the jurisdiction concerned;
- (b) obtain proof of listed status on a stock exchange; or
- (c) 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 to the AMLO.

What customer information must nonetheless be collected under SCDD²²?

4.24 When carrying out SCDD, licensees must:

- (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 licensee; and
- (c) if a person purports to act on behalf of the customer,
 - (i) identify the person and take reasonable measures to verify the person's identity; and
 - (ii) verify the person's authority to act on behalf of the customer.

APPLYING ECDD

Situations where special requirements on CDD are required

4.25 Section 15 of Schedule 2 to the AMLO provides that in a

²² Section 4(1) of Schedule 2 to the AMLO refers.

situation specified by the EAA in a written notice given to the licensee and in any other situation that by its nature may present a high risk of ML/TF, the licensee must, before establishing a business relationship or continuing an existing business relationship, among others, apply all the following ECDD measures:

- (a) obtaining approval from the senior management; and
- (b) either taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of funds that will be/are involved in the business relationship or taking additional measures to mitigate the risk of ML/TF.

4.26 High-risk situations for which ECDD apply include:

- (a) customer not physically present for identification purposes;
- (b) customer or his beneficial owner being a Hong Kong PEP or Non-Hong Kong PEP (please see paragraph 4.30 below);
- (c) customer from or transaction connected with a jurisdiction that does not adopt or insufficiently adopts the FATF Recommendations;
- (d) any situation that by its nature may present a higher risk of ML/TF; and
- (e) any situation specified by the EAA in a notice given to the licensee.

Customer not physically present for identification purposes²³

4.27 Where a customer is not physically present for identification purposes, licensees will generally not be able to determine that the documentary evidence of identity actually relates to the customer they are dealing with. Consequently, the risk in respect of the customer increases.

²³ Section 9 of Schedule 2 to the AMLO refers.

- 4.28 Except for the situation specified in paragraph 4.29, in order to mitigate the risk, sections 5(3)(a) and 9(1) of Schedule 2 to the AMLO require a licensee to take additional measures. If a customer has not been physically present for identification purposes, the licensee must carry out at least one of the following measures to mitigate the risk:
- (a) further verifying the customer's identity on the basis of documents, data or information referred to in paragraph 4.16 but not previously used for the purposes of verification of the customer's identity;
 - (b) taking supplementary measures to verify information relating to the customer that has been obtained by the licensee; or
 - (c) ensuring that the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorised institution or an institution that is incorporated or established in an equivalent jurisdiction; carries on a business similar to that carried on by an authorised institution; has measures in place to ensure compliance with the requirements similar to those imposed under Schedule 2 to the AMLO; and is supervised for compliance with those requirements by authorities in that jurisdiction that perform functions similar to those of the Monetary Authority.
- 4.29 The requirements under paragraph 4.28 when a customer is not physically present for identification purposes do not apply²⁴ if the licensee has carried out the measure referred to in paragraph 4.16(d) in relation to the customer on the basis of data or information provided by a recognised digital identification system that is a reliable and independent source that is recognised by the EAA.

²⁴ Section 9(2) of Schedule 2 to the AMLO refers.

Customer or its beneficial owner being a PEP

4.30 Definitions

A. Non-Hong Kong PEPs

A (Non-Hong Kong) PEP is defined in section 1 of Schedule 2 to the AMLO as:

- (a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong:
 - (i) including 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 not including 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).

B. Close Associate

Section 1(3) of Schedule 2 to the AMLO defines a close associate as:

- (a) an individual who has close business relations with a person falling under paragraph A(a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph A(a) is also a beneficial owner; or
- (b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph A(a).

C. Hong Kong PEPs

For the purposes of the Guidelines, a Hong Kong PEP is defined as:

- (a) an individual who is or has been entrusted with a prominent public function in Hong Kong:
 - (i) including a head of government, senior politician, senior government or judicial official, senior executive of a government-owned corporation and an important political party official;
 - (ii) but not including 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 4.30B of the Guidelines).

D. Former PEPs

For the purposes of the Guidelines, a former PEP is defined as:

- (a) an individual who, being a Hong Kong PEP or Non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in any place;
- (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), 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) (please see paragraph 4.30B of the Guidelines).

4.31 Being a PEP does not, in itself, automatically mean that a person is corrupt or has been incriminated in any corruption. However, the office and position may render a PEP vulnerable to corruption.

The risk increases when the PEP is from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their government and society. This risk is even more acute where such countries do not have adequate AML/CTF standards.

- 4.32 Licensees should take reasonable measures to determine whether an individual is a PEP. If an individual is known to be a Hong Kong PEP or Non-Hong Kong PEP, licensees must apply the ECDD measures. If an individual is known to be a Former PEP, the licensees are required to perform a risk assessment to determine whether such individual poses a higher risk of ML/TF, though being a Former PEP does not, in itself, automatically pose higher risk. In any situation that the licensee assesses a Former PEP to present a higher risk of ML/TF, he must apply the ECDD measures as required.
- 4.33 Licensees that handle the proceeds of corruption, or handle illegally diverted government, supranational or aid funds, face reputational and legal risk, including the possibility of criminal charges for having assisted in laundering the proceeds of crime and the suspension or revocation of their licences. Licensees can reduce risk by conducting ECDD before establishing a business relationship with the customer and continuously monitoring where they know or suspect that the business relationship is with a PEP.
- 4.34 Use of publicly available information for assessment of PEP
- (a) Estate agency companies and senior management should 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.
 - (b) Licensees may also use publicly available information or

refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption (an example of which is Transparency International's 'Corruption Perceptions Index', which ranks countries according to their perceived level of corruption). Licensees should be vigilant where either the country to which the customer has business connections or the business/industrial sector is more vulnerable to corruption.

- 4.35 Except for the situation specified in paragraph 4.38, when licensees know that a particular customer or beneficial owner is a PEP, they must, before establishing a business relationship or continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, apply all the following ECDD measures²⁵:
- (a) obtaining approval from the 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** that will be/are involved in the business relationship; and
 - (c) applying enhanced monitoring to the business relationship in accordance with the assessed risk.
- 4.36 A licensee should adopt reasonable measures, in accordance with his assessment of the risk, for establishing 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

²⁵ Sections 5(3)(b) and 10 of Schedule 2 to the AMLO refer.

official's source of wealth and current business interests. Licensees should however note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing the information.

- 4.37 The person approving the licensee as referred to in paragraph 4.35(a) should take into account the advice of the CO. The more potentially sensitive a PEP is, the more senior the approving person should be.
- 4.38 With respect to a high risk business relationship with a customer who is or whose beneficial owner is a Former PEP, the ECDD measures set out in paragraph 4.35 do not apply if the licensee is satisfied that:
- (a) the customer or the beneficial owner of the customer is a Former PEP; and
 - (b) the Former PEP does not present a high risk of money laundering or terrorist financing based on appropriate risk assessment.
- 4.39 Licensees must retain a copy of the assessment and review the assessment whenever they are concerned with the activities of the customer or the beneficial owner of the customer. The risk assessment²⁶ referred to in paragraph 4.38 should take into account various risk factors, such as:
- (a) the level of (informal) influence that the individual could still exercise;
 - (b) the seniority of the position that the individual held as a Hong Kong PEP or non-Hong Kong PEP; or
 - (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the Former PEP's successor, or informally by the fact that the Former PEP

²⁶ The assessment in relation to a Former PEP who is no longer entrusted with a prominent public function should be based on an assessment of risk and not merely on prescribed time limits.

continues to deal with the same substantive matters).

Customer from a jurisdiction that does not adopt or insufficiently adopts the FATF Recommendations

4.40 Licensees should pay particular attention to:

- (a) business relationships and transactions with persons (including natural persons and legal persons) from or in jurisdictions that do not or insufficiently adopt the FATF Recommendations; and
- (b) transactions and business connected with jurisdictions assessed to be of higher ML/TF risk.

Higher risk jurisdictions

4.41 Factors which licensees may take into consideration

- (a) In determining whether a jurisdiction is one which does not adopt, or insufficiently adopts the FATF Recommendations, or may otherwise pose a higher risk, licensees should consider, among other things:
 - (i) information that may have been disseminated to licensees by the EAA;
 - (ii) whether the jurisdiction is subject to sanctions, embargoes or similar measures imposed by, for example, the Security Council of the United Nations;
 - (iii) whether the jurisdiction is identified by credible sources as lacking appropriate AML/CTF laws, regulations and other measures;
 - (iv) 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
 - (v) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.
- (b) “Credible sources” refers to well-known bodies that

generally are regarded as reputable and that make information produced by them publicly and widely available. In addition to the FATF and similar 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 and does not necessarily indicate that a jurisdiction is of higher risk.

High-risk situation specified in a Notice given by the EAA²⁷

4.42 Where the requirement is called for by the FATF (which may include mandatory ECDD or the application of counter-measures recommended by FATF) or in other circumstances which are considered to be of higher risk, the EAA may issue a notice to the licensee in respect of the situation specified in the notice to:

- (a) impose an obligation on licensees to undertake ECDD measures; or
- (b) require licensees to undertake specific counter-measures²⁸ identified or described in the notice,

and the licensee concerned must comply with such a notice. The type of measures in paragraphs (a) and (b) above would be proportionate to the nature of the risks.

Carrying out CDD by means of intermediaries

4.43 Licensees may carry out any CDD measure by means of an

²⁷ Section 15 of Schedule 2 to the AMLO refers.

²⁸ Such counter-measures may include: obtaining additional information from different sources on the customer, the beneficial owner of the customer, the purpose and intended nature of the business relationship or transaction and the source of wealth or the source of the funds; increasing the frequency of review of the existing CDD records; increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination; and evaluating the information provided by a customer from a high risk jurisdiction identified by the FATF, etc.

intermediary specified in section 18(3) of Schedule 2 to the AMLO if:

- (a) the intermediary consents in writing to be the licensee's intermediary; and
- (b) they are satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the CDD measure without delay.

However, licensees remain liable under the AMLO for a failure to carry out that CDD measure.

4.44 Section 18(3) of Schedule 2 to the AMLO provides that the specified intermediary is, among others, an accounting professional, a legal professional or a licensee who is able to satisfy the licensee that he has adequate procedures in place to prevent ML/TF. The specified intermediary may also be a lawyer, notary public, an auditor, a professional accountant in an equivalent jurisdiction or a person who carries on in an equivalent jurisdiction a business similar to that carried out by a licensee provided that such a specified intermediary is required under the law of that jurisdiction to be registered or licensed or is regulated under the law of that jurisdiction, has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO and is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of the EAA.

4.45 A licensee that carries out a CDD measure by means of an intermediary must:

- (a) 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 licensee 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; and

- (b) ensure that the intermediary will, if requested by the licensee within the period specified in the record-keeping requirements of AMLO, provide to the licensee 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.

4.46 Application of AMLO to pre-existing customers²⁹

- (a) Licensees must perform the CDD measures prescribed in Schedule 2 to the AMLO and the Guidelines in respect of pre-existing customers (with whom the business relationship was established before 1 March 2018), when:
 - (i) a transaction takes place with regard to the customer which, by virtue of the amount or nature of the transaction, is unusual or suspicious; or is not consistent with the licensee'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;
 - (ii) a material change occurs in the way in which the customer's business is operated;
 - (iii) the licensee suspects that the customer or the customer's business is involved in ML/TF; or
 - (iv) the licensee doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying

²⁹ Section 6 of Schedule 2 to the AMLO refers.

the customer's identity.

- (b) Licensees should note that the requirements for continuously monitoring under section 5 of Schedule 2 to the AMLO also apply to pre-existing customers.



Chapter 5 CONTINUOUS MONITORING OF BUSINESS RELATIONSHIP WITH CUSTOMERS

Requirements on continuous monitoring

- 5.1 Effective continuous monitoring is vital for understanding customers' activities and an integral part of effective AML/CTF systems as it helps licensees update their knowledge of their customers and detect unusual or suspicious activities.
- 5.2 Pursuant to section 5 of Schedule 2 to the AMLO, a licensee must continuously monitor the business relationship with a customer by:
- (a) reviewing from time to time documents, data and information relating to the customer that have been obtained for the purpose of complying with the CDD requirements to ensure that they are up-to-date and relevant;
 - (b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the licensee's knowledge of the customer and the customer's business, risk profile and source of funds; and
 - (c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and recording his findings in writing.

Failure to conduct continuous monitoring

- 5.3 A failure to conduct proper continuous monitoring could expose licensees to potential abuse by criminals, and may call into question the adequacy of controls, or the prudence and integrity of a licensee's management.

Aspects for licensees to identify unusual customer transactions

- 5.4 To identify unusual customer transactions, the aspects which licensees may consider include:
- (a) the nature and type of transactions (e.g. abnormal size or

- frequency, cash transactions);
- (b) the nature of a series of transactions;
- (c) the amount of the transactions, paying special attention to particularly substantial transactions;
- (d) the geographical origin/destination of a payment or receipt; and
- (e) the customer's usual pattern of activities.

Risk-based approach to continuous monitoring³⁰

- 5.5 The extent of monitoring should be commensurate with the risk profile of the customer compiled through the risk assessment. For business relationships presenting a higher risk of ML/TF, more resources should be applied to monitoring.
- 5.6 Licensees should take additional measures when monitoring business relationships which pose a higher risk (please see paragraph 4.25). High-risk business relationships will require more frequent and intensive monitoring. When monitoring high-risk business relationships, the relevant considerations may include:
- (a) whether adequate procedures or management information systems are in place to provide relevant staff (e.g. CO, MLRO, front-line staff, etc.) with timely information; and
 - (b) how the sources of funds, wealth and income for higher risk customers will be monitored and how any changes in circumstances will be recorded.
- 5.7 Additional measures when monitoring business relationship do not apply in relation to³¹:
- (a) a customer of a licensee who has not been physically present for identification purposes, if the licensee has carried out the measure referred to in paragraph 4.16(d) above in relation to the customer on the basis of data or information provided by a

³⁰ Section 5 of Schedule 2 to the AMLO refers.

³¹ Sections 5(4) and 5(5) of Schedule 2 to the AMLO refers.

recognised digital identification system that is a reliable and independent source that is recognised by the EAA; or

- (b) a customer, or the beneficial owner of a customer, of a licensee if the licensee is satisfied that:
- (i) the customer or the beneficial owner of the customer is a Former PEP; and
 - (ii) the Former PEP does not present a high risk of money laundering or terrorist financing based on appropriate risk assessment³².

5.8 There are various methods by which those objectives can be met including exception reports (e.g. large transactions exception report) and transaction monitoring systems. Exception reports might help licensees monitor their customers' operational activities.

Examination of the background and purposes of transactions

5.9 Examinations or enquiries may include asking the customer appropriate questions. Such enquiries, when conducted properly and in good faith, will not constitute tipping off³³. The results of the enquiries should be properly documented. Where there is any suspicion, a STR must be made to the JFIU (please refer to Chapter 6 of the Guidelines).

Cash transactions and transfers to third parties

5.10 Where cash transactions or transfers to third parties are being proposed by a customer and such requests do not accord with the customer's known pattern of practice, a licensee should be cautious and make relevant further enquiries. Where a licensee, having made the necessary enquiries, does not consider the cash transaction or third party transfer reasonable, he should make a STR to the JFIU (please refer to Chapter 6 of the Guidelines).

³² Please refer to paragraph 4.39 in Chapter 4 of the Guidelines with respect to appropriate risk assessment of the Former PEP.

³³ Please refer to paragraph 6.6 in Chapter 6 of the Guidelines.

Chapter 6 REPORTING SUSPICIOUS TRANSACTIONS

The requirements

- 6.1 CDD and continuous monitoring of business relationship with customers provide the basis for identifying unusual and suspicious transactions and events. Once a licensee identifies or suspects that a transaction is related to ML/TF activity, the licensee should report the transaction to JFIU.
- 6.2 The term suspicious is to be applied in its everyday, normal meaning. The courts have said that “it is a possibility that is more than fanciful”.
- 6.3 The suspicion is that the funds or property involved in the transaction is the proceeds of any crime or is linked to terrorist activity. For a person to have knowledge or suspicion, he does not have to know what sort of crime has been committed or that the funds themselves definitely arose from the criminal offence, but one or more warning signs of ML/TF, which cannot be explained by the seller or buyer, will be relevant.

Statutory requirements for reporting suspicious transactions

- 6.4 Section 25A of the DTROPO and section 25A of the OSCO make it an offence if a person fails to disclose to an authorised officer where the person knows or suspects that property represents the proceeds of drug trafficking or of an indictable offence. Likewise, section 12 of the UNATMO makes it an offence to fail to disclose knowledge or suspicion of terrorist property. Under the DTROPO, the OSCO and the UNATMO, failure to report the knowledge or suspicion carries a maximum penalty of three months’ imprisonment and a fine of \$50,000.

- 6.5 The filing of a STR to the JFIU provides the licensee a statutory defence to the offence of ML/TF in respect of the acts disclosed in the report, provided that:
- (a) the STR is made before the licensee undertakes the disclosed acts and the acts or transactions are undertaken with the consent of the JFIU; or
 - (b) the STR is made after the licensee has performed the disclosed acts or transactions and the report is made on the licensee's own initiative and as soon as it is reasonable for the licensee to do so.
- 6.6 Licensees should note that it is an offence for a person, knowing or suspecting that a disclosure has been made to the JFIU, to disclose to any other person any matter which is likely to prejudice any investigation. If a customer is told that a report has been made (commonly referred to as "tipping off"), this would prejudice the investigation and an offence would be committed. The customer's awareness of a possible STR or investigation could prejudice future efforts to investigate the suspected ML/TF operation. Therefore, if licensees form a suspicion that transactions relate to ML/TF, they should be aware of the risk of tipping off when performing the CDD process. Estate agency companies and senior management should ensure that their employees are aware of and sensitive to these issues when conducting CDD.
- 6.7 Estate agency companies and senior management should ensure sufficient guidance is given to their staff to enable them to form suspicion or to recognise the signs when ML/TF is taking place. The guidance should take into account the nature of the transactions and customer instructions that staff is likely to encounter, the type of service and the means of delivery, i.e. whether face to face or remote.

6.8 The “SAFE” approach

- (a) An effective systemic approach to identify suspicious transactions may safeguard licensees from the risk of being involved with ML/TF. Licensees may adopt, where applicable, the “SAFE” approach promoted by JFIU.
- (b) Four steps are involved in the SAFE approach:
 - (i) Screen the customer and transaction for suspicious activity indicators;
 - (ii) Ask the customers appropriate questions;
 - (iii) Find out the customer’s records; and
 - (iv) Evaluate all the above information.
- (c) Licensees are strongly advised to familiarise themselves with the “SAFE” approach. Details of the SAFE approach are available at JFIU’s website (www.jfiu.gov.hk).

When and how to report suspicious transactions to JFIU?

6.9 When a licensee knows or suspects that certain property represents the proceeds of crime or terrorist property, a disclosure must be made to the JFIU as soon as it is reasonable to do so. The use of STR proforma or the e-reporting system named Suspicious Transaction Report And Management System (“STREAMS”) to report suspicious transactions is strongly encouraged.³⁴ In the event that the subject in the disclosure is related to any ongoing investigation, it should be indicated in the STR with the provision of relevant details (e.g. case reference number, name of the investigative unit and the officer-in-charge etc.), if any. Under exceptional circumstances, an initial notification by telephone may be considered for an urgent disclosure.

6.10 The law requires that a STR be made together with any information or other matter on which the knowledge or suspicion is based. The need for prompt reporting is particularly important where a

³⁴ Please visit JFIU’s website at www.jfiu.gov.hk for the full details of the reporting methods and advice.

customer has instructed the licensee to move funds or other property, carry out significant changes to the business relationship, etc. In such circumstances, licensees should consider contacting the JFIU urgently.

- 6.11 Examples of situations that could give rise to suspicions, depending on the circumstances of each case, are provided in **Appendix E**. They are not intended to be exhaustive but only provide indications of the most basic ways in which money may be laundered.

Internal reporting

- 6.12 Estate agency companies and senior management should have measures in place to check, on an ongoing basis, that it has proper policies and procedures to test and ensure compliance with the legal and regulatory requirements. 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 their respective businesses.
- 6.13 An estate agency company's MLRO should act as a central reference point for reporting suspicious transactions. The estate agency companies and senior management should ensure that the MLRO is of sufficient status within the company, and has adequate resources, to enable the MLRO to perform his functions (please refer to paragraph 2.7 above for the major responsibilities of the MLRO).
- 6.14 A key responsibility of the MLRO is to diligently consider all vital information and report suspicious transactions or activities or suspicious attempted transactions or activities to the JFIU in accordance with the statutory requirements.



- 6.15 Estate agency companies and senior management should set up and maintain procedures to ensure that:
- (a) all staff are made aware of the identity of the MLRO and the procedures to follow when making an internal disclosure report; and
 - (b) all disclosure reports should reach the MLRO without undue delay.
- 6.16 While estate agency companies and senior management may wish to set up internal systems that allow staff to consult their 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. Since the legal obligation is to report the suspicious transaction as soon as it is reasonable to do so, the 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 the speediness, confidentiality and accessibility of the systems.
- 6.17 All suspicious activities reported to the MLRO should be documented. The report should include the details of the customer and a statement on the information giving rise to the suspicion. In urgent cases, suspicious activities may be reported verbally, e.g. over the telephone, to be followed in writing.
- 6.18 The MLRO should acknowledge receipt of the report and, at the same time, issue a reminder to the reporting staff of the risk of tipping off. The tipping-off provision also applies to circumstances where suspicion has been raised internally, but has not yet been reported to the JFIU.
- 6.19 The reporting of a suspicion in respect of a transaction or event does not mean that further suspicious transactions or events in respect of the same customer need not be reported. Further

suspicious transactions or events, whether of the same nature or different from the previous ones, should also be reported to the MLRO who should make further reports to the JFIU as appropriate.

- 6.20 When evaluating an internal report of a suspicious transaction, the MLRO should take reasonable steps to consider all relevant information, including CDD and continuous monitoring information available within the company concerning the entities to which the report relates.
- 6.21 Steps to be taken by the MLRO may include:
- (a) a review of other transaction patterns and volumes;
 - (b) reference to any previous patterns of instructions, the length of the business relationship and CDD and continuous monitoring information and documentation; and
 - (c) appropriate questioning of the customer using the systematic approach to identifying suspicious transactions as recommended by the JFIU.
- 6.22 As part of the review, other connected business relationships may need to be examined. Regarding the need to search for information concerning connected business relationships, a balance should be struck between making a timely disclosure to the JFIU as required by the law and any delays in making the disclosure that might arise from searching more relevant information. The evaluation process and the conclusion drawn should be documented.
- 6.23 If after completing an evaluation a MLRO decides that there are grounds for knowledge or suspicion of transactions related to ML/TF activity, he should file a STR to the JFIU as soon as reasonable together with the information or matters on which that knowledge or suspicion is based. If the MLRO decides not to file

a STR with JFIU, provided that the MLRO acts in good faith in concluding that there is no suspicion after taking into account all available information, it is unlikely that there will be any criminal liability for failing to report. The MLRO should keep proper records of the deliberations and actions taken to demonstrate he has acted in good faith.

Keeping of records

- 6.24 Licensees should establish and maintain a record of all ML/TF reports made to the MLRO. The record should include details of the date the report was made, the name of staff members subsequently handling the report, the results of the evaluation, whether the report eventually resulted in a STR filed with the JFIU, and information to allow the documentation relevant to the report to be located.
- 6.25 Estate agency companies and senior management should establish and maintain a register of all STRs made to the JFIU. The record should include details of the date of the disclosure, the identity of the person who made the disclosure, and information to allow the papers relevant to the STRs to be located. This register may be combined with the register of internal reports, if considered appropriate.

Chapter 7

FINANCIAL SANCTIONS, PROLIFERATION FINANCING AND TERRORIST FINANCING

Financial sanctions and proliferation financing

- 7.1 Financial sanctions decided by the Security Council of the United Nations (“UN Security Council”) prohibit making available any funds, financial assets or economic resources to or for the benefit of a designated individual or entity, as well as those acting on their behalf, at their direction, or owned or controlled by such designated individuals or entities. Licensees may refer to the lists of designated individuals and entities maintained by the UN Security Council and its Sanctions Committees. The lists are available on the webpages of the relevant Committees (<https://www.un.org/securitycouncil/>).
- 7.2 The United Nations Sanctions Ordinance, Cap. 537 (“UNSO”) empowers the Chief Executive to make regulations to implement financial sanctions imposed by the UN Security Council against certain individuals and entities. Designated individuals and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Development Bureau (<https://www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html>).
- 7.3 Under regulations made under the UNSO (for example, United Nations Sanctions (Democratic People’s Republic of Korea) Regulation, Cap. 537AE and United Nations Sanctions (Joint Comprehensive Plan of Action – Iran) Regulation, Cap. 537BV), it is an offence to make available any funds, other financial assets or economic resources to or for the benefit of certain individuals and entities, or to deal with any funds, other financial assets or economic resources belonging to, owned or controlled by certain individuals and entities, except under the authority of a licence

granted by the Chief Executive. Offenders are subject to a maximum sentence of 7 years' imprisonment and a fine of an unlimited amount.

- 7.4 It is an offence under section 4 of the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526, for a person to provide any services where he believes or suspects, on reasonable grounds, that those services may be connected to weapons of mass destruction. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.
- 7.5 The EAA may inform licensees from time to time of the designations published in the Gazette or on the website of the Commerce and Economic Development Bureau pursuant to regulations made under the UNSO (<https://www.cedb.gov.hk/en/policies/united-nations-security-council-sanctions.html>).
- 7.6 Licensees should conduct name checks of their customers and the beneficial owners in relation to the customers against the latest lists of designated individuals and entities.
- 7.7 Estate agency companies and senior management should ensure that they have an appropriate system to enable their staff to conduct name checks against the relevant lists of the designated individuals and entities and that the lists are up-to-date.

Terrorist Financing

- 7.8 According to FATF, terrorist financing is the financing of terrorist acts, terrorists and terrorist organisations. Section 7 of the UNATMO prohibits the provision or collection of property for use to commit terrorist acts. Section 8 of the UNATMO prohibits any person from making available or collecting/soliciting property or

financial (or related) services for terrorists and terrorist associates. Section 8A of the UNATMO prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate. Section 11L of the UNATMO prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the penetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).

- 7.9 The UN Security Council has also published the names of individuals and organisations subject to financial sanctions in relation to involvement with Al-Qa'ida, ISIL (Da'esh) and the Taliban. All United Nations member states are required to freeze the funds and other financial assets or economic resources of any person(s) named in the lists and to report any suspected name matches to the relevant authorities.
- 7.10 According to section 6 of the UNATMO, 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 property except under the authority of a licence granted by the S for S. Contraventions are subject to a maximum penalty of 7 years' imprisonment and a fine.
- 7.11 The S for S may grant a licence to enable the property mentioned in paragraph 7.10 be dealt with.
- 7.12 Except under the authority of a licence granted by the S for S, it

is an offence:

- (a) to make any property or financial (or related) services available, by any means, directly or indirectly, to or for the benefit of a terrorist or terrorist associate;
- (b) to collect property or solicit financial (or related) services, by any means, directly or indirectly, for the benefit of a terrorist or terrorist associate; and
- (c) to deal with, directly or indirectly, any property which is specified terrorist property or property of a specified terrorist or terrorist associate.

7.13 Contraventions are subject to a maximum sentence of 14 years' imprisonment and a fine.

7.14 Licensees may also refer to additional sources of information such as the designations made by the US Government under the relevant Executive Orders.

7.15 Licensees should conduct name checks of their customers and the beneficial owners in relation to the customers against the latest lists of terrorist suspects.³⁵

7.16 Estate agency companies and senior management should ensure that they have an appropriate system to enable their staff to conduct name checks against the relevant lists of terrorist suspects and that the lists are up-to-date.

³⁵ "A Terrorist List in the Gazette" of the list of names of persons designated as terrorists or terrorist associates published in the Gazette is available at the website of JFIU (www.jfiu.gov.hk).

Chapter 8 RECORD-KEEPING

The requirements³⁶

- 8.1 Record-keeping is an integral part of the AML/CTF systems as it provides an audit trail for the detection, investigation and confiscation of criminal or terrorist property or funds. Record-keeping helps investigating authorities establish the profile of a suspect, trace the criminal's or terrorist's property or funds and assists the court to examine all relevant transactions to assess whether the property or funds are the proceeds of or relate to criminal offences or terrorist activities.
- 8.2 Licensees should maintain all relevant records of customers, transactions, etc. that are necessary and sufficient to meet the record-keeping requirements under the AMLO, the Guidelines and other relevant regulatory requirements.
- 8.3 The record-keeping requirements in respect of **each customer** are as follows:
- (a) Licensees must keep the original or a copy of:
 - (i) the documents, and a record of the data and information obtained in the course of identifying and verifying the identity of
 - the customer;
 - beneficial owner of the customer; and
 - the person who purports to act on behalf of the customer; and
 - (ii) the files relating to the customer's business relationship and business correspondence³⁷ with the customer and any beneficial owner of the customer; and
 - (b) The documents and records mentioned in sub-paragraph (a)

³⁶ Sections 20 and 21 of Schedule 2 to the AMLO refer.

³⁷ Licensees are not expected to keep each and every correspondence, such as a series of emails with the customer, the expectation is that sufficient correspondence is kept to demonstrate compliance with the AMLO.

above must be kept throughout the continuance of the business relationship with the customer and for a period of at least **five years** beginning on the date on which the business relationship ends. For an occasional transaction that is carried out in the circumstances as mentioned in paragraph 4.6(b) above, the documents must be kept for a period of at least **five years** beginning on the date on which the occasional transaction is completed.

- 8.4 The record-keeping requirements in respect of **each transaction** are as follows:
- (a) Licensees must keep the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, which may include a copy of the provisional agreement for sale and purchase; and
 - (b) Records required to be kept under sub-paragraph (a) must be kept for a period of at least **five years** beginning on the date on which the transaction is completed, regardless of whether the business relationship ends during the period.

Manner in which records are to be kept

- 8.5 If the record consists of a document, either the original of the document must be retained or a copy of the document must be kept on microfilm or in the database of a computer. If the record consists of data or information, such record must be kept either on microfilm or in the database of a computer.
- 8.6 Under section 20(4) of Schedule 2 to the AMLO, the EAA may, by notice in writing to a licensee, require the licensee to keep the records relating to a specified transaction or customer for a specified period that is longer than those referred to in paragraphs 8.3 and 8.4, where the records are relevant to an ongoing criminal or other investigation, or any other purposes as specified in the notice.

- 8.7 A licensee to whom a notice is given under section 20(4) of Schedule 2 to the AMLO must keep the relevant records for the period specified in the notice.

Chapter 9

STAFF AWARENESS AND TRAINING

- 9.1 Staff training is an important element of an effective system to prevent and detect ML/TF activities. The effective implementation of AML/CTF systems, even if they are well designed, may be compromised if the staff using the systems are not adequately trained.
- 9.2 In conducting awareness and training programmes on the effective implementation of AML/CTF systems, estate agency companies and senior management should be mindful of the following:
- (a) staff should be trained in what they need to do to perform their respective roles with respect to AML/CTF;
 - (b) estate agency companies and senior management should implement a clear and well-articulated policy for ensuring that relevant staff receives adequate AML/CTF training, and in this regard, a policy manual is useful to raise staff awareness and for reference between training sessions;
 - (c) training methods and assessment should be determined according to the size and complexity of the business and the type and level of ML/TF risk; and
 - (d) the frequency of training should be sufficient for the staff to maintain their AML/CTF knowledge and competence.
- 9.3 Staff members should be made aware of:
- (a) the licensee's statutory obligations and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROPO, the OSCO and the UNATMO;
 - (b) any other statutory and regulatory obligations that concern the licensee and themselves under the AMLO, the DTROPO, the OSCO, the UNATMO and the UNSO, and the possible

consequences of breaches of these obligations;

- (c) the estate agency company's policies and procedures relating to AML/CTF, 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 perform their respective roles with respect to AML/CTF.

9.4 Focused training for appropriate staff or groups of staff will enable estate agency companies and senior management to implement their AML/CTF systems effectively. The following areas of training may be appropriate for certain groups of staff :

- (a) All new staff (irrespective of seniority)
 - (i) an introduction to the background of ML/TF and the importance of AML/CTF to the licensee; and
 - (ii) the need and obligation to identify and report suspicious transactions to the MLRO, and the offence of "tipping-off".
- (b) Front-line staff (i.e. staff dealing with customers directly)
 - (i) the importance of their roles in the estate agency company's AML/CTF strategy being the first point of contact with potential money launderers and persons involved in TF;
 - (ii) the estate agency company's policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities;
 - (iii) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and
 - (iv) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be

required.

- (c) Back-office staff
 - (i) appropriate training on customer verification and the relevant processing procedures; and
 - (ii) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.
- (d) Managerial staff (including internal audit staff and CO)
 - (i) higher level training covering all aspects of Hong Kong's AML/CTF regime;
 - (ii) specific training in the AML/CTF requirements applicable to licensees; and
 - (iii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as the reporting of suspicious transactions to the JFIU.
- (e) MLRO
 - (i) specific training in relation to the MLRO's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and
 - (ii) training to keep abreast of AML/CTF requirements/developments generally.

9.5 Depending on the learning needs of their staff, estate agency companies and senior management are encouraged to consider using a mix of training techniques and tools in delivering training. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as procedural manuals. Estate agency companies and senior management may consider including available FATF publications and typologies as part of the training materials. All materials should be up-to-date and in line with current requirements and standards.



- 9.6 Estate agency companies and senior management should monitor the effectiveness of the training. This may be achieved by:
- (a) testing staff's understanding of the estate agency company's policies and procedures to combat ML/TF, their understanding of relevant statutory and regulatory obligations, and also their ability to identify suspicious transactions; and
 - (b) monitoring the compliance of staff with the estate agency company's AML/CTF 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.

Appendix A

ACRONYMS, TERMS AND ABBREVIATIONS	
Acronyms / terms / abbreviations	Meaning
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
AML/CTF	Anti-money laundering and/or counter-terrorist financing
AML/CTF systems	The policies, procedures and controls developed and implemented for AML/CTF purposes
CDD	Customer due diligence
CO	Compliance officer
DTROPO	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
EAA	Estate Agents Authority
EAO	Estate Agents Ordinance (Cap. 511)
ECDD	Enhanced customer due diligence
Estate agency company(ies)	A business entity(ies) (whether a company, partnership or sole proprietorship) which is a licensed estate agent under the Estate Agents Ordinance.
FATF	Financial Action Task Force
Individual	Individual means a natural person, other than a deceased natural person
JFIU	Joint Financial Intelligence Unit
Licensee(s)	Holder(s) of an Estate Agent's Licence (Individual), Estate Agent's Licence (Company) or a Salesperson's Licence (as the case may be) granted under the Estate Agents Ordinance
MLRO	Money laundering reporting officer
ML/TF	Money laundering and/or terrorist financing
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)



ACRONYMS, TERMS AND ABBREVIATIONS	
Acronyms / terms / abbreviations	Meaning
PEP(s)	Politically exposed person(s)
Proliferation financing or PF	Financing of proliferation of weapons of mass destruction
RBA	Risk-based approach
SCDD	Simplified customer due diligence
Senior management	means a chief executive officer, managing director, sole proprietor, managing partner, directors (or board), senior managers or other operating management personnel (as the case may be) who is/are a licensed estate agent(s) under the Estate Agents Ordinance and who is/are responsible, either individually or collectively, for the control, management and/or supervision of an estate agency company's business
STR(s)	Suspicious transaction report(s), also referred to as reports or disclosures
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)

Examples of the specific factors in relation to ML/TF risk rating

For assessing the ML/TF risk rating of a customer, the following are some of the specific factors for consideration:

A. In relation to the customer

- (a) is the customer a natural person or a legal person;
- (b) does the customer have a complex ownership structure, for example:
 - using multiple companies or trusts which adds layers of complexity to ownership;
 - using multiple intermediaries or professionals to hide ownership or to arrange unusually complicated transactions;
 - or
 - is the customer an overseas seller or buyer especially from a high risk jurisdiction identified by the FATF;
- (c) unusual involvement of apparently unconnected third parties, particularly where the buyer appears to have a low income;
- (d) is the customer or his beneficial owner an individual in public positions and/or locations that carry a higher exposure to the possibility of corruption, including PEP;
- (e) is the customer or his beneficial owner a designated individual or entity subject to financial sanctions; and
- (f) is the customer or his beneficial owner a terrorist suspect.

B. In relation to the transaction

- (a) are any payment(s) of the deposit(s) in cash, and:
 - buyers carrying out large one-off cash transaction; or
 - a large cash deposit with balance from an unusual source;
- (b) are the payments of the deposit(s) made to or received from third parties:
 - a third party, apparently unconnected with the seller or buyer, bearing the costs, settling invoices or otherwise paying the



transaction costs;

- the customer requesting payment to a third party who has no apparent connection with the customer; or
 - proceeds of a sale sent to a high risk jurisdiction or unknown third party;
- (c) multiple payments of smaller amounts possibly through different accounts and to avoid thresholds put in place by overseas authorities;
- (d) unusual speed or request to expedite transactions unnecessarily possibly over or under value;
- (e) sale price significantly above or below market price; and
- (f) the immediate resale (flipping) of property at a higher value.

C. Others

- (a) is the seller or buyer a non face-to-face customer;
- (b) where multiple properties are purchased, resold or exchanged;
- (c) an unknown third party appears at a late stage;
- (d) a sudden or unexplained change in ownership within a short period of time;
- (e) the licensee is asked to hold a big sum in its client account, then refund it to the same or a different account; and
- (f) successive transactions, especially of the same property, with unexplained changes in value.

Appendix C

Identification and verification of customer (including beneficial owner) who is an individual

1. Information of a customer and/or his beneficial owner to be collected include:
 - (a) Full name;
 - (b) Date of birth;
 - (c) Identity document type and number; and
 - (d) Address (*post office box address is not acceptable*).

2. Licensees should obtain the following documents for verification of the information as stated in paragraph 1 above and retain a copy of the documents for record keeping:
 - (a) Hong Kong residents:
 - Hong Kong identity card for permanent residents;
 - Birth certificate of a minor (*i.e. a person who has not attained the age of 18 years*) not in possession of a valid travel document or Hong Kong identity card (the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified); or
 - Travel document (*a copy of the "biodata" page should be retained*).
 - (b) Non-residents:
 - A valid travel document;
 - A relevant national identity card (issued by government) bearing the person's photograph;
 - A valid national driving licence (issued by government) bearing the person's photograph; or
 - Where customers do not have a travel document or a national identity card or driving licence with a photograph, licensees 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.

3. Travel Documents

Travel documents include a passport or some other document which contains a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder. The following documents are regarded as 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) Exit-entry Permit for Travelling to and from Hong Kong and Macau for Official Purposes; and
- (f) Exit-entry Permit for Travelling to and from Hong Kong and Macau.

4. The standard identification requirement is likely to be sufficient for most situations. If, however, the customer and/or his beneficial owner is assessed to present a higher ML/TF risk, a licensee should consider whether he should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

5. If the beneficial owner of the customer is one in relation to a partnership or trust, please refer to paragraph 4.18(d) and (e) in Chapter 4 of the Guidelines.



Appendix D

**Identification and verification of customer (including beneficial owner)
which is a corporation**

1. Information of a customer to be collected include:
 - (a) full name of the corporation;
 - (b) date and place of incorporation;
 - (c) registration or incorporation number;
 - (d) address of registered office in the place of incorporation (*post office box address is not acceptable*);
 - (e) name(s) of the current director(s);
 - (f) name(s) of the current shareholder(s); and
 - (g) where it comes to the knowledge of a licensee that the current shareholder(s) is/are not the beneficial owner(s) of the customer, name(s) of the beneficial owner(s).

2. The above-mentioned information should be obtained as a standard requirement. If, however, the customer and/or its beneficial owner(s) is assessed to present a higher ML/TF risk, a licensee should consider whether he should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

3. For a corporation incorporated in Hong Kong, i.e. a company incorporated under the Companies Ordinance (Cap. 622), the information of the company as stated in paragraph 1 above can usually be verified against the information in the Companies Register maintained by the Companies Registry. A licensee should verify such information by conducting a search at the Companies Registry and obtaining, for example, a company search report (e.g. an annual return) and other image records of documents of the company filed at the Companies Registry, copies of which must be retained for record keeping.

4. For a corporation incorporated outside Hong Kong, the information of the corporation as stated in paragraph 1 above can usually be verified against:
- (a) a company search report issued by the company registry in the place of incorporation or a similar or comparable document to a company search report; or
 - (b) a certificate of incumbency or equivalent issued by the registered agent in the place of incorporation or a copy thereof certified by a professional third party in the relevant jurisdiction; or
 - (c) any other written evidence issued by the government or an official authority in the place of incorporation.

A licensee should obtain from the customer any of the documents as stated in this paragraph and retain a copy of the same for record keeping.

5. If the relevant information of the company as stated in paragraph 1 above cannot be verified by documents mentioned in paragraphs 3 or 4 above (e.g. if no company search is conducted or if the relevant documents have not been filed or could not be produced), a licensee should obtain from the customer a copy certified by a professional third party of the following documents and retain a copy of the same for record keeping:
- (a) the certificate of incorporation;
 - (b) a list showing the name(s) of all the current director(s) and current shareholder(s) of the company; the address of its registered office; and
 - (c) a list showing the name(s) of all the beneficial owner(s) of the customer, if appropriate.

Definition of “beneficial owner” in relation to a corporation

6. Section 1 of Schedule 2 to the AMLO defines beneficial owner in

relation to a corporation as:

- (a) an individual who –
 - (i) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;
 - (ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or
 - (iii) exercises ultimate control over the management of the corporation; or
 - (b) if the corporation is acting on behalf of another person, means the other person.
7. A licensee should identify and record the identity of all beneficial owners and take reasonable measures to verify the identity of the beneficial owners. For the guidance on the identification and verification of a beneficial owner, please refer to **Appendix C**.
8. For companies with multiple layers in their ownership structures, whether incorporated in or outside Hong Kong, the intermediate layers of the companies should all be identified. The manner in which this information is collected should be determined by the licensee by, for example, obtaining a director's declaration annexing an ownership chart describing the intermediate layers (the information to be included should be determined on a risk sensitive basis but should at least include the company name and place of incorporation). The objective should always be to follow the chain of ownership to the individuals who are the beneficial owners of the direct customer of the licensee and verify the identity of those individuals. For the avoidance of doubt, in order to complete the CDD measures for companies with multiple layers in their ownership structures, apart from verifying the identity of the beneficial owners of the customer, licensees should also verify the information of each intermediate layer of the companies. Please

refer to paragraphs 1 to 5 above (as appropriate) for ways to carry out the verification of customer (including beneficial owner(s)) which is a corporation.

9. Where the ownership is dispersed, the licensee should concentrate on identifying and taking reasonable measures to verify the identity of those who exercise ultimate control over the management of the company.
10. If the beneficial owner of the customer is one in relation to a partnership or trust, please refer to paragraph 4.18(d) and (e) in Chapter 4 of the Guidelines.



Appendix E

Examples of situations that could give rise to suspicions, depending on the circumstances of each case, include but not limited to the following:

- (a) checking the customer's identity is difficult;
- (b) the customer is reluctant to provide details of his identity or provides fake documents;
- (c) the customer being evasive or reluctant to provide required CDD information or documentation or where ownership is said to be confidential;
- (d) the customer is trying to use intermediaries to protect his identity or hide his involvement;
- (e) need to go through several legal entities in order to identify the beneficial owner or being unable to identify whether there are any beneficial owners;
- (f) non-HK resident using intermediaries where it makes no commercial sense;
- (g) no apparent reason for using the licensee's services, for example, another business is better placed to handle the size of the transaction;
- (h) searches on the customer show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery;
- (i) part or full settlement in cash or foreign currency, with weak reasons;
- (j) the customer is keen to buy or sell quickly at an unusually low or high price for no legitimate reasons;
- (k) cash exchanges directly between seller and buyer;
- (l) poor explanation for the early redemption of a previous mortgage, especially where redemption incurs a heavy penalty cost;
- (m) the customer does not take up services that are attractive or is willing to pay fees that seem unnecessary;
- (n) the property value does not fit the customer's profile;
- (o) the buyer has not viewed the property despite viewing is possible



- or has only seen it on the internet;
- (p) the ownership is not transparent and uses complex trusts, offshore arrangements or multiple companies;
 - (q) for an existing customer, there has been a significant or unexpected improvement in the customer's financial position and the customer cannot give a proper explanation of where money came from or provide their source of wealth or funds;
 - (r) a third party, apparently unconnected with the seller or buyer, bears the costs, or otherwise pays the transaction costs;
 - (s) the buyer will not disclose the source of the funds where required;
 - (t) unusual involvement of third parties, or large payments from private funds, particularly where the buyer appears to have a low income;
 - (u) unusual source of funds;
 - (v) the customer provides an address that is unknown or believed to be false;
 - (w) the buyer purchases multiple properties in a short period of time and seems to have little concern about the location and condition, etc. of each of the property;
 - (x) the customer is based in jurisdictions subject to a call by the FATF or in countries where the production of drugs or drug trafficking may be prevalent; and
 - (y) unusual use of new technologies not used in the normal course of business.