P. GUIDELINES ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING

CONTENTS

ANNEXURE

P. GUIDELINES ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING

A. TABLE OF MANDATORY REQUIREMENTS

Mandatory Requirements	
1. Client identification and verification	▪ **Objective**:- Take reasonable measures to obtain basic information on the identity of the client, and in an Applicable Circumstance (as defined in paragraph 25 of this Practice Direction), verify the client's identity. Client identification and verification are two distinct concepts. Identification refers to the basic information a solicitor is required to obtain and record about his clients to know who they are whenever he is retained: their names, addresses, telephone numbers, occupation, etc. Verification refers to the information a solicitor needs to obtain to confirm that his clients are who or what they say they are. ▪ **Applicable situations**:- Client identification is required in all cases including cases for the same client. Client verification is only required when a solicitor is acting for a client (new or existing) or giving instructions on behalf of such client in any of the Applicable Circumstances as defined in paragraph 25 of this Practice Direction, i.e. any one of the situations (i) to (vi) set out in this Section A item 2 (Client due diligence) below. ▪ **When**:- (i) Establishing business relationship; or (ii) Carrying out occasional transactions; (iii) In exceptional or urgent circumstances where it is not practicable to verify client's identity before accepting instructions (as, for example, if it is necessary not to interrupt the normal conduct of business) and any risk of money laundering or terrorist financing that may be caused by carrying out the verification procedure after accepting the instruction is effectively managed, verification should be made as soon as practicable after accepting the instructions. ▪ **How**:- to conduct identification and verification is set out in paragraphs 104 – 115.
2. Client due diligence	▪ **Applicable situations**:- When acting for a client (new or existing) in any of the following activities:- (i) Financial transactions (e.g. buying and selling of real estate, business, company, securities and other assets and property) (ii) Managing client money[1], securities or other assets; (iii) Management of bank, savings or securities accounts; (iv) The formation, structure, re-organisation, operation or management of companies and other entities and legal arrangements; (v) Insolvency cases and tax advice; (vi) Other transactions involving custody of funds as stakeholder or escrow agent or transfer of funds through their bank accounts.

[1] Simply operating a solicitor's client account would not generally be regarded as "managing client money". However, where a solicitor handles money under the terms of a power of attorney for a client, it may be considered as "managing client money".

	▪ **How**:- (i) Obtain information on the nature and intended purpose of the transaction; (ii) Obtain information on the business relationship between the client and other interested parties to the transaction; (iii) Obtain information on the source of funding; (iv) Where appropriate, check client's and beneficial owner's name against the United Nations sanctions list and the list of terrorists or terrorist associates[2]; and (v) Assess money laundering and terrorist financing risks associated with a new or existing client by taking into account various factors such as client risk, country risk, service risk, transaction and delivery channels risk to apply appropriate and proportionate client due diligence and risk mitigating measures. **Firms should adopt a risk-based approach in determining the level of information to be obtained.**
3. Enhanced client due diligence	▪ **Applicable situations**:- (i) When handling complex, unusually large transactions, or an unusual pattern of transactions, which have no apparent economic or lawful purpose; or (ii) When acting for clients considered as "high risk", for example (without limitation):- - Overseas companies where corporate information is not readily accessible or with nominee shareholders/directors or a significant portion of capital in the form of bearer shares; or - Non-Hong Kong and other high-risk politically exposed persons ("**PEPs**") and persons, companies and government organisations related to them; or - Persons or entities from or in non-cooperative countries and territories ("**NCCT**")[3] identified by the Financial Action Task Force ("**FATF**")[4] or such other jurisdictions known to have insufficiently complied with FATF Recommendations; (iii) When preliminary interview leads to:- - Suspicion of money laundering, terrorist or proliferation financing; or - Doubt about the veracity or adequacy of previously obtained client identification data. or

[2] Where a client is a legal person, a trust or other similar legal arrangement, consideration should be given to identify all the connected parties of the client by obtaining their names and screen against PEP lists, the United Nations sanctions list and the list of terrorists or terrorist associates subject to a risk-based approach.

A connected party of a client that is a legal person, a trust or other similar legal arrangement:
(a) in relation to a corporation, means a director of the client;
(b) in relation to a partnership, means a partner of the client;
(c) in relation to a trust or other similar legal arrangement, means a trustee (or equivalent) of the client; and in other cases not falling within subsection (a), (b) or (c), means a natural person holding a senior management position or having executive authority in the client.

[3] The current list of NCCTs can be found on the FATF website.

[4] The FATF was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of crime through the financial system. Hong Kong has been a full member of FATF since March 1991 and has the obligation to implement the FATF Recommendations, which include the 40 Recommendations of the FATF on Money Laundering and the 9 Special Recommendations of FATF on Terrorist Financing. The current list of FATF Members and Observers can be found on the FATF website.

	(iv) Where the Government through the Law Society has issued notices informing Members of situations which may present a high risk of money laundering or terrorist financing. ▪ **How:-** Conduct enhanced due diligence as set out in paragraphs 122 – 125.
4. Politically exposed person (Non-Hong Kong PEP)	▪ **A non-Hong Kong PEP means**:- (a) an individual who is or has been entrusted with a prominent public function outside Hong Kong and (i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official; (ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), 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). ▪ **A close associate means:-** (i) an individual who has close business relations with a person falling under paragraph (a), including an individual who is a beneficial owner of a legal person or trust of which the person falling under paragraph (a) is also a beneficial owner; or (ii) 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). When a solicitor knows that a client or a beneficial owner of a client is a non-Hong Kong PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship where the client or the beneficial owner is subsequently found to be a non-Hong Kong PEP, apply enhanced due diligence measures set out in paragraph 124. In determining what constitutes a prominent (public) function, solicitor should consider on a case-by-case basis, taking into account various factors, including but not limited to: (a) the powers and responsibilities associated with a particular public function; (b) the organisational framework of the relevant government or international organisation; and (c) any other specific concerns connected to the jurisdiction where the public function is/has been entrusted.
5. Politically exposed person (Hong Kong PEP)	▪ **A Hong Kong PEP means**:- (a) an individual who is or has been entrusted with a prominent public function in Hong Kong and (i) includes head of government, senior politician, senior government, or judicial official, or senior executive of a government-owned corporation and an important political party official;

	(ii) but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i); (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), or a spouse or a partner of a child of such an individual; or (c) a close associate of an individual individual falling within paragraph (a).
6. Politically exposed person (International Organisation PEP)	▪ **An international organisation[5] PEP means**:- (a) an individual who is or has been entrusted with a prominent function by an international organisation, and (i) includes members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions; (ii) but does not include a middle-ranking or more junior official of the international organisation; (c) 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 (d) a close associate of an individual falling within paragraph (a).
7. Enhanced client due diligence measures for Hong Kong and International Organisation PEPs	Solicitors should take reasonable measures to determine whether a client or a beneficial owner of a client is a Hong Kong or an international organisation PEP and assess money laundering/terrorist financing risks to determine whether the client or or a beneficial owner of the client pose a higher risk of money laundering/terrorist financing. Hong Kong or international organisation PEP status in itself does not automatically confer higher risk. Solicitors should apply the enhanced due diligence measure set out in paragraph 124 in situation where the Hong Kong or the internal organisation PEP presents a higher risk of money laundering/terrorist financing taking into account all risk factors, including those set out in paragraph 121 that are relevant to the business relationship.
8. Treatment of former Hong Kong, Non-Hong Kong and International Organisation PEPs (former PEPs)	▪ **A former PEP means**:- (a) an individual who has been but is not currently entrusted with a prominent public function; (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)

[5] International organisations are entities established by formal political agreements between their member states that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organization; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organization or the Association of Southeast Asian Nations, etc.

	Following a risk-based approach, solicitors may decide not to apply or continue to apply the enhanced client due diligence measures set out in paragraph 124 to a client who is, or whose beneficial owner is, a former PEP. Such decision can only be made with the approval of the senior management and on the basis that the PEP no longer presents a high risk of money laundering/terrorist financing. To determine whether a former PEP no longer presents a high risk of money laundering/terrorist financing, solicitors should conduct an appropriate assessment on the money laundering/terrorist financing risk associated with the PEP status, taking into account various risk factors, including but not limited to: (a) the level of (informal) influence that the individual could still exercise; (b) the seniority of the position that the individual held as the PEP; and (c) whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters).
9. Simplified client due diligence (SDD)	Solicitors may apply SDD measures to clients and products presenting a low money laundering/terrorist financing risk as defined in section 4, Division 1, Part 2, Schedule 2 to the AMLO. SDD measures should not be applied or continue to be applied, where: (a) a client or transaction presents high risk of money laundering/terrorist financing as defined in the *Table of mandatory requirements under Section A, item 3 (Enhanced client due diligence)*; (b) the risk assessment changes during the course of business; (c) there is a suspicion of money laundering/terrorist financing; or (d) where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification. SDD measures in relation to beneficial owners: (a) a solicitor may choose not to identify and take reasonable measures to verify the beneficial owner in relation to client or products listed in section 4, Division 1, Part 2, Schedule 2 to the AMLO; (b) if a client not falling within the scope of section 4, Division 1, Part 2, Schedule 2 to the AMLO has in its ownership chain an entity that falls within the scope of section 4 Division 1, Part 2, Schedule 2 to the AMLO, it is not necessary to identify or verify the beneficial owners of that entity in that chain when establishing a business relationship. However, solicitors should still identify and take reasonable measures to verify the identity of beneficial owners in the ownership chain that are not connected with that entity; (c) where a client is a corporation listed on any stock exchange, solicitors may choose not to identify and take reasonable measures to verify its beneficial owners only if the public company is subject to disclosure requirements (either by stock exchange rules, or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership of the client;

	(d) where a client is an investment vehicle[6], solicitors may choose not to identify and take reasonable measures to verify its beneficial owners (i.e. the investors) where the person responsible for carrying out the client due diligence measures in relation to all the investors of the investment vehicle is: (i) a Financial Institution as defined in the AMLO; (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction, which has measures in place to ensure compliance with requirements similar to those set out in the Schedule 2 to the AMLO, and is supervised for compliance with those requirements. (e) an investment vehicle whether or not responsible for carrying out client due diligence measures on the underlying investors under the governing law of the jurisdiction in which the investment vehicle is established may, where permitted by law, appoint another institution ("appointed institution"), such as a manager, a trustee, an administrator, a transfer agent, a registrar or a custodian, to perform the client due diligence. Where the person responsible for carrying out the client due diligence measures (the investment vehicle or the appointed institution) falls within any of the categories of institution set out in section 4(3)(d) of Schedule 2 to the AMLO, solicitors may choose not to identify and take reasonable measures to verify the beneficial owners of the investment vehicle provided that it is satisfied that the investment vehicle has ensured that there are reliable systems and controls in place to conduct the client due diligence (including identification and verification of the identity) on the underlying investors in accordance with the requirements similar to those set out in the Schedule 2 to the AMLO. (f) if neither the investment vehicle nor appointed institution fall within any of the categories of institution set out in section 4(3)(d) of Schedule 2 to the AMLO, solicitors should identify any investor owning or controlling more than 25% interest of the investment vehicle. The solicitors may consider whether it is appropriate to rely on a written representation from the investment vehicle or appointed institution (as the case may be) responsible for carrying out the client due diligence stating, to its actual knowledge, the identities of such investors or (where applicable) there is no such investor in the investment vehicle. This will depend on risk factors such as whether the investment vehicle is being operated for a small, specific group of persons. Where solicitors accept such a representation, this should be documented, retained, and subject to periodic review. For the avoidance of doubt, solicitors are still required to take reasonable measures to verify those investors owning or controlling more than 25% interest of the investment vehicle and (where applicable) other beneficial owners in accordance with Annexure 8.

[6] An investment vehicle may be in the form of a legal person or trust, and may be a collective investment scheme or other investment entity.

	Examples of possible SDD measures include: (a) accepting other documents, data or information (e.g. proof of Financial Institution's license, listed status or authorization status); (b) adopting SDD measures in relation to beneficial owners as described above; (c) reducing the frequency of updates of client's identification information; (d) reducing the degree of ongoing monitoring; or (e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and intended nature from the type of transactions or business relationship established.
10. Timing for conducting client due diligence	▪ **When:-** (i) Establishing a solicitor / client relationship; or (ii) Carrying out occasional transactions; (iii) In exceptional or urgent circumstances where it is not practicable to conduct client due diligence at the time of instructions, due diligence should be done as soon as practicable after preliminary client identification. **Nevertheless, law firms should determine the risks involved in acting for a client considered as "high risk" before completing due diligence.** (iv) Ongoing review is required for any client considered as "high risk", or where there are changes to instructions or a relationship between a client and relevant party(ies) which give rise to suspicions.
11. Record keeping	Files including records for client identification and due diligence should be kept for the period as follows:- (i) Conveyancing matters - 15 years; (ii) Tenancy matters - 7 years; (iii) Other matters, except criminal cases - 7 years; and (iv) Criminal cases - 5 years from expiration of any appeal period. Records of a transaction which is subject to a suspicious transaction report and investigation should be kept until the relevant authority has confirmed that the case has been closed.
12. Staff awareness and training	(i) Make the Guidelines and the firm's internal policies and procedures (as supplemented and updated from time to time) available to new and existing employees; and (ii) Provide ongoing training to staff on how to recognise and deal with suspicious transactions and to keep them up-to-date on relevant legal provisions and on trends of money laundering, terrorist and proliferation financing techniques.

B. INTRODUCTION

13. In July 2004, the Law Society set up a Working Party on Anti-Money Laundering to consider the impact of the revised Forty Recommendations in relation to measures against money laundering developed by the FATF. Given the complexity and importance of the issues, the Working Party was converted into a full Committee in November 2004. In late 2006, the Law Society on the recommendation of the Committee on Anti-Money Laundering resolved to publish a comprehensive set of Guidelines relating to anti-money laundering and terrorist financing for use by law firms, solicitors and foreign lawyers practising in Hong Kong.

14. These Guidelines supersede Circular 97-280, Circular 03-428, Circular 05-291 (SD) and Circular 18-647 (SD) on money laundering and terrorist financing:

15. These Guidelines apply to all law firms, solicitors and foreign lawyers practising in Hong Kong and aim to:-

    15.1 provide general guidance on the subjects of anti-money laundering, terrorist financing, financial sanctions and proliferation financing

    15.2 summarise the relevant legislative provisions on anti-money laundering, terrorist financing, financial sanctions and proliferation financing;

    15.3 require compliance by practitioners of prescribed requirements to prevent money laundering, terrorist and proliferation financing;

    15.4 offer useful general guidelines to law firms for developing their own procedures on anti-money laundering, terrorist and proliferation financing appropriate to their businesses; and

    15.5 highlight issues which would affect the practice of law in Hong Kong.

16. These Guidelines do not have the force of law and should not be interpreted as such. However, where provisions are specified as mandatory herein (currently paragraphs 21 – 33), any law firm, solicitor or foreign lawyer practising in Hong Kong that fails to comply with such provisions may face disciplinary action (see Chapter 15 of The Hong Kong Solicitors' Guide to Professional Conduct ("**Guide to Professional Conduct**"). In addition, firms which do not comply with these Guidelines will be exposed to additional risks of being involved in money laundering and terrorist financing activities, with severe consequences of criminal prosecution and significant loss of reputation.

17. These Guidelines will be kept under review and revised from time to time.

C. LEGISLATION ON MONEY LAUNDERING, TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING

18. Legislation concerned with money laundering, terrorist financing, financial sanctions and financing of proliferation of weapons of mass destruction:-

    18.1 Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("**AMLO**");

    18.2 Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("**DTRPO**");

    18.3 Organized and Serious Crimes Ordinance (Cap. 455) ("**OSCO**");

18.4 United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("**UNATMO**");

18.5 United Nations Sanctions Ordinance (Cap. 537) ("**UNSO**"); and

18.6 Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526) ("**WMD(CPS)O**").

19. It is important for solicitors to raise their awareness of these provisions and to comply with them to minimise the risk of becoming involved inadvertently in criminal offences such as:-

19.1 assisting persons known or suspected to be laundering money generated by drug trafficking or any indictable offence, or providing or collecting funds used to commit terrorist acts or making funds available to terrorists or terrorist associate(s);

19.2 failing to report a suspicious case of money laundering or terrorist financing;

19.3 tipping off clients who were subject to investigation for an offence of money laundering or terrorist financing;

19.4 failing to comply with court orders for the purpose of investigation of crime and to make information available;

19.5 make available any funds or other financial assets or economic resources to, or for the benefit of, designated persons or entities under the UNSO, as well as those acting on their behalf, at their direction, or owned or controlled by them; or to deal with any funds, other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities; or

19.6 provide any services where it is believed or suspected, on reasonable grounds, that those services will or may assist the development, production, acquisition or stockpiling of Weapons of Mass Destruction ("WMD") in Hong Kong or elsewhere.

20. Summaries on the key provisions of the DTRPO, OSCO, UNATMO, UNSO and WMD(CPS)O are set out in **Annexure 2**.

D. BASIC POLICIES AND PROCEDURES REQUIRED OF LAW FIRMS

21. In support of the international initiatives to combat money laundering, terrorist and proliferation activities, there is a need for awareness and vigilance on the part of legal practitioners and their staff. Law firms should therefore have in place appropriate policies and procedures of internal control for identifying and (where appropriate) reporting suspicious transactions. With the implementation of AMLO on 1 March 2018, law firms are required to comply with the provisions of this Ordinance.

Mandatory Requirements

22. Every law firm carrying on business in Hong Kong is required to comply with the requirements outlined in paragraphs 21 – 33 below when they act for clients in any matter.

Client identification, verification and due diligence

23. As a basic requirement, law firms must make reasonable efforts to identify and, in an Applicable Circumstance, verify the true identity of all clients (new or existing) requesting the firm's services. Each firm should carefully consider whether financial transactions should be conducted with clients who fail to provide satisfactory evidence of their identities. Recommended procedures and policies on client identification and verification are set out in paragraphs 104 – 115.

24. In general, law firms should satisfy themselves with the identity of the client and the beneficial owner(s)[7] of a client which is not a natural person at the time of the instruction. In exceptional or urgent circumstances where this is not reasonably practicable, the verification procedure should be made as soon as practicable after the preliminary identification.

25. In addition to the basic client identification and verification measures, law firms are required to carry out different levels of client due diligence as set out in the *Table of mandatory requirements under Section A* when instructed to act in any of the following activities (referred to therein as the "Applicable Circumstances"; and any one of them an "Applicable Circumstance"):-

    25.1 financial transactions such as buying and selling of real estate, business, company, securities and other assets and property;

    25.2 managing client money, securities or other assets;

    25.3 management of bank, savings or securities accounts;

    25.4 the formation, structure, re-organisation, operation or management of companies and other entities and legal arrangements;

    25.5 insolvency cases and tax advice;

    25.6 other transactions involving custody of funds by law firms as stakeholder or escrow agent or transfers of funds through their bank accounts.

26. The timing required for conducting client due diligence is similar to that required for client identification and verification (i.e. at the time of the instruction and before accepting the instruction). However, in exceptional or urgent circumstances where this is not practicable, it would be permissible to have the due diligence process completed as soon as practicable after accepting the instruction. Nevertheless, **where the client is considered as "high risk", the firm should carefully determine the risks involved in acting for such client before completing the due diligence process**.

27. Where a solicitor is unable to verify the identity of a client or is suspicious of the relevant transaction after conducting due diligence, the solicitor should carefully evaluate the risks involved and determine whether he should continue to act for the client and, if appropriate, report any suspicion on money laundering or terrorist financing activities to an authorized officer. In this respect, care must be taken to ensure that he would not inadvertently commit the offence of tipping off (see paragraphs 79 – 80 and 90 – 91).

Record keeping

28. Law firms should also make reasonable efforts in keeping the records of their existing clients updated from time to time and conducting periodic reviews on the risk profile of the clients.

[7] See the definition of beneficial owner in Annexure 8.

29. All files, including all documents relating to the transactions and records obtained or compiled for client identification and due diligence, should be retained in order to facilitate the retrieval of information relating to client identification and due diligence. The recommendations contained in the existing Circular 12-475 should be observed. The retention period for the following types of transactions is as follows:-

29.1 conveyancing matters – 15 years;

29.2 tenancy matters – 7 years;

29.3 other matters, except criminal cases – 7 years; and

29.4 criminal cases – 5 years from expiration of any appeal period.

The above retention periods also apply to copies of the individual client's identification documents including the Hong Kong identity cards and passports collected in relation to the files or transactions.

30. Such records should be kept in such a way that the law firm can swiftly comply with any information requests from a competent authority.

31. Records of a transaction which is the subject of a suspicious transaction reporting and investigation should be kept until the relevant authority has confirmed that the case has been closed.

Staff Awareness and Training

32. These Guidelines and the firm's internal policies and procedures (as supplemented and updated from time to time) are to be made available to new and existing employees to raise awareness of money laundering, terrorist and proliferation financing, financial sanctions and facilitate recognition and (where appropriate) reporting of suspicious transactions.

33. Further, each law firm has to provide ongoing training to staff on recognition, reporting and handling of suspicious transactions and on the updated legislation and trends of money laundering, terrorist and proliferation financing techniques.

Recommended Measures

34. Solicitors are reminded that the effort in combating money laundering, terrorist and proliferation financing does not end at the point of accepting instructions and care must be taken at all times to identify suspicious transactions. Examples of suspicious transaction indicators and risk areas are provided in **Annexure 4**.

35. Law firms should develop and implement policies and procedures of internal control appropriate to the nature and scope of their business for identifying and (where appropriate) reporting money laundering, terrorist and proliferation financing.

36. In establishing such policies and procedures, law firms should take a risk-based approach. The guiding principle is that objective reasonable steps should be taken to detect and prevent money laundering, terrorist and proliferation financing activities and transactions. It is prudent for law firms to keep written records of the steps taken by them. They are required to make their own independent assessment taking into consideration the circumstances of each case. Recommended procedures and policies for recognition and reporting of suspicious transaction are provided in **Annexure 5**. A standard report form is at www.jfiu.gov.hk.

37. Such procedures should be communicated in writing to all solicitors and staff of the firm and be reviewed and updated on a regular basis to ensure their effectiveness.

38. Law firms should co-operate with law enforcement authorities to the extent permitted by law or contractual obligations relating to client confidentiality.

New services, new business practices and use of new technologies

39. Law firms should identify and assess the money laundering and terrorist financing risks that may arise in relation to:

    39.1 the development of new services and new business practice(s), including new delivery mechanisms; and

    39.2 the use of new or developing technologies for both new and pre-existing services.

40. Law firms should undertake the risk assessment prior to the launch of the new service, new business practice, or the use of new or developing technologies, and should take appropriate measures to manage and mitigate the risks identified.

41. Law firms should also consider conducting a periodic firm-wide risk assessment depending on the size and complexity of the law firm to identify, assess and understand how and to what extent it is vulnerable to money laundering, terrorist and proliferation financing risks. To determine the appropriate level and type of mitigation, a documented firm-wide risk assessment should take into account:

    (a) the size of the law firm;

    (b) type of clients;

    (c) jurisdictions or countries its clients are from;

    (d) services it provides; and

    (e) type of transactions and delivery channels.

E. RELEVANT LEGAL ISSUES

Legal Professional Privilege ("LPP")

42. Special privilege from disclosure, known as LPP, is rendered to communications made:-

    42.1 between a legal adviser and his client for the purpose of giving legal advice to the client; and

    42.2 between a legal adviser and his client and any other person in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

43. LPP does not exist for communications or documents which are held with the intention of furthering a criminal purpose.

44. In recognition of the LPP under common law, there are provisions in the DTRPO, OSCO and UNATMO[8] exempting items subject to LPP from the disclosure requirements therein.

[8] Section 2(14) of DTRPO, section 2(18) of OSCO and section 2(5) of UNATMO.

45. Interpretive Note to Recommendation 23 of The 40 Recommendations of the FATF on Money Laundering also provides that:-

"Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege."

46. Nevertheless, where a solicitor, through information subject to LPP, becomes aware or suspicious that a transaction being handled by him involves criminal or terrorist activities in contravention of the DTRPO, OSCO or UNATMO, he should consider if it remains appropriate for him to continue to act for the relevant client.

47. If the solicitor considers there is a conflict of interest or does not wish to continue to act, he should cease to act for that client. **It is therefore advisable for law firms to include a standard clause in their engagement letters to the effect that the firm may terminate its relationship with the client at any time if it is of the opinion that a conflict of interest arises,** whether the conflict is between clients of the firm or between the client and the firm.

Client Confidentiality

48. Solicitors are required to comply with Rule 8.01 of the Guide to Professional Conduct which provides:-

"A solicitor has a legal and professional duty to his client to hold in strict confidence all information concerning the business and affairs of his client acquired in the course of the professional relationship, and must not divulge such information unless disclosure is expressly or impliedly authorised by the client or required by law or unless the client has expressly or impliedly waived the duty."

49. Such general duty of confidentiality may, in certain circumstances, be overridden by orders of the court. For example, an order made pursuant to section 4 of the OSCO, which requires the production of particular material (other than that subject to legal professional privilege) which is relevant for the purpose of an investigation into an organized crime or proceeds of crime.

50. Where a solicitor becomes aware or suspicious that a client's transaction may relate to money laundering or terrorist financing and that the information he has does not fall within LPP, he should consider carefully whether a report should be made to an authorized officer or he may be held liable for failing to make disclosure as required by the DTRPO, OSCO or UNATMO.

51.1 If the solicitor determines that a report should be made, a conflict of interest may arise between him and the client. In these circumstances, the solicitor should consider carefully whether he should continue to act for the client.

51.2 The statutory protections under section 25A(3) of the OSCO, section 25A(3) of the DTRPO and section 12(3) of the UNATMO should also be considered. These subsections (which are identical) read as follows:

"A disclosure referred to in subsection (1) [i.e. a report]-

(a) shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision;

(b) shall not render the person who made it liable in damages for any loss arising out of-

(i) the disclosure;

(ii) any act done or omitted to be done in relation to the property concerned in consequence of the disclosure."

52. When a report has been made, the solicitor should not disclose to the client or any third party the making of such report, otherwise the solicitor may commit the offence of "tipping off".

53. The standard clause recommended to be incorporated into a law firm's engagement letter with its client under the above paragraph 47 is particularly useful in circumstances where a report has been made to the authority so that the law firm may terminate the solicitor/client relationship without giving information which may make it liable for the offence of tipping off.

Litigation

54. There are provisions under the DTRPO, OSCO and UNATMO imposing criminal liability on persons (i) having knowledge of or suspicion on money laundering and/or terrorist financing activities and (ii) entering into or becoming involved in such activities, unless disclosure is made and consent to continue with the involvement is obtained from an authorized officer (the "**Relevant Provisions**"). Details of these provisions are provided in **Annexure 2**.

55. Solicitors may in the course of representing clients in existing or contemplated legal proceedings become aware of or suspicious that the subject matter of the proceedings relates to money laundering or terrorist financing activities, or enter into or become involved in such activities. Solicitors in these situations may be at risk of being caught by the Relevant Provisions.

56. In circumstances where the relevant information was obtained from one's own client, disclosure would be exempted by reason of LPP set out in paragraph 42 above.[9]

57. The position is less clear where the relevant information was obtained as a result of discovery made by the opposing party. Based on the decision of the English Court of Appeal in **Bowman v Fels** [2005] EWCA Civ 226, in the absence of clear language, the disclosure obligation imposed by the Relevant Provisions would not override the implied undertaking of lawyers not to use documents disclosed in the discovery procedure of a legal proceeding to any third party or for other purpose. Further, the English Court of Appeal expressed the view that the function of litigation is to resolve the rights and duties of two parties according to law and therefore the conduct of legal proceedings would not be regarded as "carrying out" a "transaction" relating to money laundering. It therefore appears that the Relevant Provisions would not apply to solicitors conducting genuine legal proceedings for their clients. This proposition however is yet to be tested before the Hong Kong Courts.

58. If the solicitor considers there is a conflict of interest or does not wish to continue to act, he should not accept any further instructions from the client.

Civil liability

59. Section 25A(3) of DTRPO and OSCO and section 12(3) of UNATMO expressly provide that the making of disclosure under section 25A(2) of DTRPO and OSCO and section 12(2) of UNATMO respectively shall not be treated as breach of contract or confidentiality and the person making such disclosure shall not be made liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

[9] See also paragraph 77.

60. These exemptions from liability in damages, however, do not prevent a party adversely affected by the disclosure made pursuant to the relevant legislation, to make other civil claims such as constructive trusteeship, money had and received and tracing in equity.

Confidentiality Agreement

61. Commercial solicitors are often required by clients (particularly corporate clients) to enter into confidentiality agreements before the clients disclose information relating to their transactions. To ensure that they are not deprived of the protection of section 25A(3) of the DTRPO and OSCO and section 12(3) of UNATMO, solicitors should be cautious in entering into confidentiality agreements **subject to foreign law**. Further, solicitors should be cautious when required by clients to confirm that clients' information will remain confidential, as such representations could be considered to be misleading.

F. DISCLAIMER

62. Notwithstanding the recommendations made by the Law Society, these Guidelines are not intended to provide legal advice. Practitioners are required to form their own opinions on each individual case.

ANNEXURE 1

What are money laundering and terrorist financing?

63. Money laundering is a transaction or a series of transactions effected with the aim to conceal or change the identity of criminal proceeds, so that the money, after such processing, will appear to have originated from a legitimate source.

64. "Money laundering" is defined in Part 1 of Schedule 1 to AMLO to mean 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.

65. Similar to money laundering, terrorist financing also aims at disguising the origin of funds, but its focus is on the directing of funds, whether legitimate or not, to terrorists. It is defined in Part 1 of Schedule 1 to AMLO to mean

(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.

66. There are 3 common stages of money laundering:-

66.1 *Placement* - the introduction of criminal proceeds into the financial system. Law firms are at risk of getting involved by dealing with client money.

66.2 *Layering* - after the criminal proceeds are placed into the financial system, complex transactions are effected to disguise the audit trail and obscure the origin of the funds.

66.3 *Integration* - if the layering process succeeds, the criminal proceeds will reappear in the financial system as legitimate funds and assets.

Law firms are at risk of being targeted to assist in transactions such as the purchase or sale of property which may be a part of placement, layering or integration in a money laundering scheme. The offence of "dealing" in section 2 of DTRPO and OSCO is set out in paragraph 75 of **Annexure 2** of this Practice Direction.

67. There is an increasing sophistication of techniques used by criminals in laundering funds including the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and the increased use of professionals to provide advice and assistance in laundering criminal funds. Particular attention should be paid when cash is received from clients. Proceeds of many crimes are often generated in the form of cash. As law firms receive and deal with client money on daily basis, they are increasingly targeted as a route to placing cash into the financial system.

ANNEXURE 2

Summary on key provisions in the DTRPO, OSCO and UNATMO

Key Provisions under DTRPO and OSCO (collectively the "Ordinances")

Failure to disclose

68. Section 25A(1) of the Ordinances imposes a duty on a person, who knows or suspects that any property:-

    (a) in whole or in part directly or indirectly represents any person's proceeds of;

    (b) was used in connection with; or

    (c) is intended to be used in connection with,

    drug trafficking or an indictable offence, to disclose that knowledge or suspicion, together with any matter on which that knowledge or suspicion is based, to an authorized officer as soon as it is reasonable for him to do so.

69. It should be noted that references to an indictable offence in sections 25 and 25A of OSCO include conduct which would constitute an indictable offence if it had occurred in Hong Kong. Accordingly, it is an offence for a person to deal with the proceeds of crime or fail to make the necessary disclosure although the principal crime is not committed in Hong Kong provided that it would constitute an indictable offence if it had occurred in Hong Kong. Similarly references to drug trafficking in sections 25 and 25A of DTRPO include drug trafficking committed outside Hong Kong.

70. An "authorized officer", as defined under section 2 of the Ordinances, includes:-

    (a) any police officer;

    (b) any member of the Customs and Excise Service; and

    (c) any other person authorized by the Secretary for Justice for the purposes of the Ordinances including any officer in the Joint Financial Intelligence Unit ("**JFIU**")[10].

71. Failure to make a disclosure under section 25A(1) is an offence and the penalties upon conviction are imprisonment for 3 months and a fine at level 5 (currently at HK$50,000).

72. Section 25A(3) of the Ordinances provides that such disclosure shall not be treated as a breach of any restriction on disclosure imposed by contract, enactment or rule of conduct and the person making such disclosure shall not be made liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

73. Section 25A(4) of the Ordinances further extends the provisions of section 25A to disclosure made by an employee to an appropriate person in accordance with the procedure established by his employer for the making of such a disclosure. This provides protection to employees of a law firm against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to the person designated by their employer.

[10] The JFIU is operated jointly by the Police and the Customs and Excise Service

Active money laundering

74. Section 25(1) of the Ordinances makes it an offence for a person to deal with any property which he, knowing or having reasonable grounds to believe that such property in whole or in part directly or indirectly represents any person's proceeds of drug trafficking or of an indictable offence respectively.

75. "Dealing" is defined under section 2 of the Ordinances to include:-

(a) receiving or acquiring the property;

(b) concealing or disguising the property (whether by concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect of it or otherwise);

(c) disposing of or converting the property;

(d) bringing into or removing from Hong Kong the property;

(e) using the property to borrow money, or as security (whether by way of charge, mortgage or pledge or otherwise).

76. The penalties for these offences are, on indictment 14 years imprisonment and a fine of HK$5,000,000 and on summary conviction, 3 years imprisonment and a fine of HK$500,000.

77. Section 25(2) of both Ordinances provides that it is a defence for a person charged with an offence under section 25(1) to prove that:-

(a) he intended to disclose such knowledge, suspicion or matter to an authorized officer; and

(b) there is reasonable excuse[11] for his failure to make disclosure in accordance with section 25A(2).

78. Further, section 25A(2) of both Ordinances provides that if a person who has made the necessary disclosure does any act in contravention of section 25(1) and the disclosure relates to that act, he does not commit an offence if:-

(a) that disclosure is made before he does that act and the act is done with the consent of an authorized officer; or

(b) that disclosure is made after he does that act on his initiative and as soon as it is reasonable for him to make it.

Tipping off

79. Section 25A(5) of the Ordinances makes it an offence for a person, knowing or suspecting that a disclosure has been made under section 25A, to disclose to any other person any matter which is likely to prejudice any investigation which might be conducted following the first-mentioned disclosure.

80. The penalties for the offence are, upon indictment a fine of HK$500,000 and imprisonment for 3 years and on summary conviction, a fine at level 6 (currently at HK$100,000) and imprisonment for 1 year.

[11] The existence of common law legal professional privilege constitutes a "reasonable excuse" for not reporting and as a defence to the principal offence of money laundering. See paragraphs 44 and 45 of these Guidelines.

Key Provisions under UNATMO

Failure to disclose

81. Section 12 of the UNATMO provides that where a person knows or suspects that any property is terrorist property, then the person shall disclose to an authorized officer the information or other matter:-

(a) on which the knowledge or suspicion is based; and

(b) as soon as is practicable after that information or other matter comes to the person's attention.

82. Section 2 of the UNATMO provides definitions to the following:-

"Authorized officer" – (a) a police officer; (b) a member of the Customs and Excise Service; (c) a member of the Immigration Service; or (d) an officer of the Independent Commission Against Corruption.

"Terrorist" – a person who commits, or attempts to commit, a terrorist act or who participates in or facilitates the commission of a terrorist act.

"Terrorist act" – the use or threat of action where (i) the action is carried out with the intention of, or the threat is made with the intention of using action that would have the effect of (A) causing serious violence against a person; (B) causing serious damage to property; (C) endangering a person's life, other than that of the person committing the action; (D) creating a serious risk to the health or safety of the public or a section of the public; (E) seriously interfering with or seriously disrupting an electronic system; or (F) seriously interfering with or seriously disrupting an essential service, facility or system, whether public or private; and (ii) the use or threat is (A) intended to compel the Government or to intimidate the public or a section of the public; and (B) made for the purpose of advancing a political, religious or ideological cause.

"Terrorist associate" – an entity owned or controlled, directly or indirectly, by a terrorist.

"Terrorist property" – (a) the property of a terrorist or terrorist associate; or (b) any other property consisting of funds that was used or is intended to be used to finance or otherwise assist the commission of a terrorist act.

83. A list of designated terrorist, terrorist associates and terrorist properties is from time to time published in the Gazette. Section 5(4) of the UNATMO provides that in the absence of evidence to the contrary, it shall be presumed that persons or properties specified in such a list are terrorists, terrorist associates or terrorist properties.

84. Section 14 of UNATMO provides that the maximum penalty for failure to make disclosure under section 12 is imprisonment for 3 months and a fine at level 5 (currently at HK$50,000).

85. Similar to section 25A(3) of the Ordinances, section 12(3) of the UNATMO provides that the making of the required disclosure shall not be treated as a breach of contract or enactment or rule of conduct which restricts disclosure and shall not render the person who made the disclosure liable in damages therefor.

86. Similar to section 25A(4) of the Ordinances, section 12(4) of UNATMO renders protection to employees against the risk of prosecution where they have made disclosure to an appropriate person in accordance with the procedure established by their employers.

Active terrorist financing

87. Section 7 of the UNATMO prohibits a person from providing or collecting, by any means, directly or indirectly, funds:-

(a) with the intention that the funds be used; or

(b) knowing that the funds will be used,

in whole or in part, to commit one or more terrorist acts (whether or not the funds are actually so used).

88. Section 8 of the UNATMO prohibits any person, except under the authority of a licence granted by the Secretary for Security, from making any funds or financial (or related) services available, directly or indirectly, to or for the benefit of a person he knows or has reasonable grounds to believe is a terrorist or terrorist associate.

89. Under section 12(2), it is a defence against prosecution under section 7 or 8 if a person who has made a disclosure under section 12(1) does any act before or after the disclosure and :-

(a) that disclosure is made before the person does that act and the person does that act with the consent of an authorized officer; or

(b) that disclosure is made after the person does that act on the person's initiative and as soon as it is practicable for the person to make it.

Tipping off

90. Section 12(5) of the UNATMO prohibits a person who knows or suspects that a disclosure has been made from disclosing to another person any information or other matter which is likely to prejudice any investigation which might be conducted following the first-mentioned disclosure.

91. Any person found guilty of the offence under section 12(5) shall be liable on conviction on indictment to a fine and to imprisonment for 3 years and on summary conviction to a fine at level 6 (currently at HK$100,000) and to imprisonment for 1 year.

Other Provisions under the Ordinances and UNATMO

92. In addition to the above offences under the Ordinances and UNATMO, such Ordinances also confer extensive powers on the authorities to carry out investigation on drug trafficking, organized crimes and terrorist activities, including the production of materials and furnishing of information (other than those subject to legal professional privilege) and authority to search premises, with an order of the court. Failure to comply with such order or hindrance of the relevant authority in execution of such order may amount to criminal liability. There are also provisions imposing criminal liability on persons committing acts which may prejudice investigation.

Financial Sanctions and Proliferation Financing

Financial Sanctions

93. The UNSO provides for the imposition of sanctions against persons and against places outside the People's Republic of China arising from Chapter 7 of the Charter of the United Nations. Most United Nation Security Council Resolutions ("UNSCR") are implemented in Hong Kong under the UNSO.

94. The UNSO empowers the Chief Executive to make regulations to implement sanctions decided by the United Nations Security Council ("UNSC"), including targeted financial sanctions[12] against certain individuals and entities, such as those designated by the UNSC or its Committees. Designated persons and entities are specified by notice published in the Gazette or on the website of the Commerce and Economic Department Bureau ("CEDB").

Except under the authority of a licence granted by the Chief Executive, it is an offence:

(a) to make available, directly or indirectly, any funds, or other financial assets, or economic resources, to, or for the benefit of:

(i) designated persons or entities;

(ii) persons or entities acting on behalf or, at the direction of designated persons or entities; or

(iii) entities owned or controlled by the aforementioned; or

(b) to deal with, directly or indirectly, any funds, or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities.

95. The Chief Executive may grant a licence for making available any funds, or economic resources to, or dealing with any funds or other financial assets or economic resources belonging to, or owned or controlled by, certain persons or entities under specified circumstances in accordance with the provisions of the relevant regulation made under the UNSO. Solicitors seeking such licence should write to the CEDB.

96. Section 3 of the UNSO provides that the maximum penalty for a contravention or breach of financial sanctions on summary conviction is 2 years and a fine of HK$500,000, and on indictment, imprisonment for 7 years and an unlimited fine.

97. Lists of persons and entities subject to financial sanctions under the UNSO are available on the websites of the UNSC and CEDB.

12 Targeted financial sanctions refer to both asset freezing and prohibitions to prevent funds, other financial assets or economic resources from being made available to, directly or indirectly, or for the benefit of certain persons and entities.

Proliferation financing

98. FATF defines "**proliferation financing**" as:

> "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".

99. FATF Recommendation 7 requires countries to implement targeted financial sanctions to comply with the UNSCRs relating to the prevention, suppression and disruption of proliferation of weapon of mass destruction and its financing.

100. To combat proliferation financing, the UNSC adopts a two-tiered approach through resolutions made under Chapter VII of the UN Charter imposing mandatory obligations on UN member states:

(a) global approach under UNSCR 1540 (2004) and its successor resolutions; and

(b) country-specific approach under UNSCR 1718 (2006) against the Democratic People's Republic of Korea (DPRK) and UNSCR 2231 (2015) against the Islamic Republic of Iran (Iran) and their successor resolutions.

101. The counter proliferation financing regime is implemented in Hong Kong through the targeted financial sanctions against Democratic People's Republic of Korea and Iran under the WMD(CPS)O and the following two UNSO regulations, namely the:

(a) United Nations Sanctions (Democratic People's Republic of Korea) Regulation (Chapter 537AE); and

(b) United Nations Sanctions (Joint Comprehensive Plan of Action—Iran) Regulation (Chapter 537BV).

102. Section 4 of the WMD(CPS)O prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to weapons of mass destruction proliferation in or outside Hong Kong. The provision of services is widely defined and includes the lending of money or other provision of financial assistance as well as the provision of professional services.

103. Providing services that will or may assist the development, production, acquisition or stockpiling of weapons of mass destruction is an offence and the penalties on summary conviction is imprisonment for 2 years and a fine of HK$500,000, and on indictment, imprisonment for 7 years and an unlimited fine.

ANNEXURE 3

Client identification, verification and due diligence

Client identification and verification

104. In general, reasonable measures must be taken:-

104.1 to identify the client;

104.2 in an Applicable Circumstance, to verify the identity of the client by using reliable and independent source documents, data or information; and

104.3 for companies and other legal entities, to identify and, in an Applicable Circumstance, verify the persons who have effective control or beneficial ownership of the company or legal entity.

105. **Original documents** (e.g. identity card or passport of an individual, certificate of incorporation or registration of a company or other legal entity) should be inspected whenever possible for verification purpose. Where originals are not available, copies of such documents from a reliable independent source (e.g. copies certified by appropriately regulated professional) should be obtained. Where verification and client due diligence are required, law firms, solicitors and foreign lawyers are required to take or collect copies of individual client's identification documents. Individual client's identification documents include Hong Kong identity cards and passports. Copies of all such documents must be kept as a record. It is also advisable to note down when the original document(s) was/were inspected and when the copy(ies) was/were taken.

Individuals

106. For clients who are individuals, reasonable measures must be taken to obtain and, in an Applicable Circumstance, verify the following information:-

106.1 name;

106.2 number of identification document, such as identity card or passport;

106.3 address, as confirmed by documents such as a recent utility bill or bank statement;

106.4 occupation or business.

Companies

107. The separate entity of a company makes it an attractive form to money launderers. It is important for solicitors acting for corporate clients to have sufficient knowledge on the background of such clients. For corporate clients, reasonable measures must be taken to:-

107.1 identify the person purporting to give instructions on behalf of the client and, in an Applicable Circumstance, verify his identity;

107.2 verify that such person is duly authorized, e.g. obtaining a copy of the company's board resolution which evidenced the conferring of authority on the person concerned;

107.3 obtain proof on the legal status of the client, such as a certificate of incorporation, information recorded at the public register such as the Companies Registry, Business Registration Office, the register of authorized institutions of the Monetary Authority and the register of licensed companies of the Securities and Futures Commission, identity of directors and/or trustees, office address and constitutive documents such as Memorandum and Articles of Association;

107.4 identify and understand the beneficial ownership and control structure of the client and, in an Applicable Circumstance, take reasonable steps to verify the identity of persons having such ownership or control.

108. In determining what constitutes reasonable steps to verify the identity of a beneficial owner or persons having ultimate ownership or control over the client, solicitors should take into account the money laundering/terrorist financing risks posed by the client, and consider whether it is appropriate to make use of the records of a beneficial owner available in the public domain (e.g. the significant controllers register), request its client to provide documents or information in relation to the beneficial owner's identity obtained from a reliable and independent source, or corroborate the client's undertaking or declaration with publicly available information.

Power of Attorney and Agency

109. When a solicitor acts for an attorney or agent of another person, reasonable measures must be taken to obtain the identity and, in an Applicable Circumstance, verification documents of both the attorney/agent and the principal. Enquiry must be made on the relationship between the attorney/agent and the principal.

110. Solicitors should inspect the original document conferring the authority on the person giving instruction, such as the original Power of Attorney or letter of appointment of the agent, and obtain a copy of it. Where originals are not available, copies of such documents from a reliable independent source (e.g. copies certified by an appropriately regulated professional) should be inspected and copied.

Estates

111. When acting for an estate, the client would be the executor(s) or administrator(s) of that estate. The identity of such individual/legal entity will have to be verified by appropriate measures applicable to an individual or legal entity as provided above. In addition, the following document(s) should be obtained:-

111.1 Death certificate; and

111.2 (where appropriate) Grant of probate or letters of administration.

Trust arrangements

112. Complex trust arrangement is a common form used by criminals to shield their money laundering or terrorist financing activities, for the ownership of the underlying trust property is not apparent. Where the client itself or the transaction to be undertaken involves trust arrangements, the firm must take reasonable steps to identify all parties involved, including the trustee, settlor and beneficial owners, and, in an Applicable Circumstance, verify their identities accordingly.

113. Enquiries should be made to understand the nature of the trust.

114. A copy of the trust deed should be obtained.

Charities

115. Charities may be used as a vehicle of money laundering and terrorist financing in that donations received from donors are apparently applied for charitable purposes. When accepting instructions from an existing charity, a copy of the charity's constitution, trust deed or Memorandum and Articles of Association must be obtained and, in an Applicable Circumstance, its status verified from reliable independent source such as conducting a search at the Companies Registry. Reasonable measures, in an Applicable Circumstance, must be taken to verify the identity of the individuals having effective control of the charity.
In setting up charities for clients, in addition to the client identification and verification procedures, solicitors should carefully assess the purpose of the charity and consider if there are indicators that donations could be directed to an organization with a suspicious background.

Non-face to face relationship

116. Due to the increasing money laundering threat of using new or developing technology that favours anonymity, special attention must be paid to non-face to face business relationships or transactions, or if a client refuses to meet face to face without a good reason.

117. In such a situation, copies of identification documents certified by qualified persons, such as solicitors or accountants, should be obtained if possible. If certified documents cannot be obtained, law firms should attempt to verify the identity of the clients by alternative means (e.g. obtain information through a credit reference agency or information service provider). In any event, the law firm must satisfy itself that the evidence so obtained is reasonably capable of establishing that the client is the person he claims to be. Section 18, Division 4, Part 2 of Schedule 2 to the AMLO provides for carrying out of client due diligence by means of specified intermediaries (see paragraph 118 below). Alternatively, funds should be remitted through a bank in Hong Kong or an equivalent jurisdiction.

Instructions referred by intermediaries

118. Law firms may rely on client identification and verification conducted by specified intermediaries (including an overseas office of the firm) in respect of clients referred by them, provided that the following are satisfied:-

118.1 the specified intermediary is adequately regulated or supervised, and has appropriate measures in place to comply with the client identification and verification requirements (e.g. banks, other law firms or professionals such as accountants); and

118.2 copies of the client identification and verification documents must be obtained from the specified intermediary and kept as a record. Where the intermediary is an overseas office of the firm, the firm may choose not to obtain copies of such documents if they are readily available from the overseas office upon request but the client identity information must be obtained.

118.3 the categories of specified intermediaries are contained in section 18, Division 4, Part 2, Schedule 2 to the AMLO.

IMPORTANT

119. Although solicitors may rely on client information provided by a specified intermediary, **they will not be absolved from potential liability** in connection with money laundering or terrorist financing as the ultimate responsibility to establish client identity remains with them.

Client due diligence

120. When acting for a client (new or existing) in any financial transaction or any activity involving custody, management or transfer of funds or assets, or management of companies or other entities, insolvency cases or tax advice, reasonable measures must be taken to conduct client due diligence to:-

120.1 obtain information on the nature and intended purpose of the transaction(s) to be undertaken;

120.2 obtain information on the business relationship between the client and other interested parties to the transaction(s);

120.3 obtain information on the source of funding of the client;

120.4 where appropriate, check client's and beneficial owner's name against the United Nations sanctions list and the list of terrorists or terrorist associates; and

120.5 assess money laundering and terrorist financing risks associated with a new or existing client by taking into account various factors such as client risk, country risk, service risk, transaction and delivery channels risk to apply appropriate and proportionate client due diligence and risk mitigating measures.

121. The extent of client due diligence may vary from client to client, depending on the type of client, business relationship and the transaction to be undertaken. When determining the risk profile of a client, the following factors should be taken into account:-

121.1 client risk factor, for example:
(i) the client or the beneficial owner of the client is a PEP;
(ii) cash intensive/higher risk sector or business;
(iii) the ownership structure of the corporate client or legal arrangement appears unusual or excessively complex given the nature of the corporate client's or legal arrangement's business; involves shell vehicle(s), nominee shareholders/directors or bearer shares; or
(iv) the client is seeking anonymity.

121.2 country risk factor, client or beneficial owner of the client is from or located in:
(i) non-cooperative countries and territories identified by the FATF, or such other jurisdictions known to have insufficiently complied with FATF Recommendations;
(ii) countries or jurisdictions having a significant level of corruption;
(iii) countries or jurisdictions subject to sanctions, embargos or similar measures implemented by the United Nations; or
(iv) countries, jurisdictions or geographical areas that have designated organization operations or strong links to terrorist activities.

121.3 transaction or delivery channel risk factors, for example:
(i) value and complexity of the transaction;
(ii) involvement of cash payment(s);
(iii) the geographical origin/destination of a payment or receipt; or
(iv) payment(s) received from or instructed to be credited to a third party unassociated with the transaction.

121.4 service risk factor - legal services which may attract a higher level of money laundering /proliferation or terrorist financing risk;

121.5 purpose of the transaction to be undertaken; and

121.6 other information that may suggest that the client is of high money laundering or terrorist financing risk.

Enhanced client due diligence

122. Where enhanced due diligence is required in applicable situations or in respect of clients considered as "high risk", additional measures must be applied by solicitors, including:-

122.1 requiring approval from the management or senior partner to establish the business relationship or to continue an existing business relationship; and

either

122.2 taking reasonable measures to establish the relevant client's or beneficial owner's source of wealth and the source of funds that will be involved in the business relationship; or

122.3 taking additional measures to mitigate the risk of money laundering and terrorist financing involved (e.g. by obtaining and verifying further details on the transaction(s) to be undertaken, their underlying purpose and parties involved); and

122.4 conducting enhanced on-going monitoring of the business relationship.

123. The further enquiry/investigation and findings made by the solicitor must be kept on record. Documents verifying that information must also be obtained and kept on record.

Enhanced client due diligence measures for politically exposed person

124. In relation to Non-Hong Kong and other high-risk PEPs and persons, companies and government organisations clearly related to them, additional measures must be taken by solicitors including:-

124.1 taking reasonable measures to establish the source of wealth and source of funds of such persons;

124.2 requiring approval from the management or a partner of the firm before accepting instructions; and

124.3 conducting enhanced on-going monitoring of the business relationship with such persons.

125. Since not all PEPs pose the same level of money laundering risks, solicitors should adopt a risk-based approach in determining the extent of enhanced due diligence measures in paragraph 124 taking into account factors such as:

125.1 the nature of the prominent (public) functions that a PEP holds;

125.2 the geographical risk associated with the jurisdiction where a PEP holds prominent (public) functions;

125.3 the nature of the business relationship (e.g. the delivery/distribution channel used; or the service offered); and

125.4 if the PEP is a former PEP, the risk factors specified in the *Table of mandatory requirements under Section A, item 8 (Treatment of former Hong Kong, Non-Hong Kong and International Organisation PEPs).*

ANNEXURE 4

Examples of suspicious transaction indicators and risk areas

Suspicious transaction indicators

126. The following are some examples of suspicious transaction indicators:-

126.1 unusual settlement requests - such as settlement by cash in large transactions for the purchase of property; or payment by way of third-party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor without justification or apparent reason;

126.2 unusual instructions (e.g. where the relevant client has no discernable reason for using the firm's services such as when an overseas client could find the same service in his country of residence); or clients whose requirements do not fit into the normal pattern of the firm's business and could be more easily serviced elsewhere;

126.3 large sums of cash to be held in client account, either pending further instructions from the client or for no other purpose than for onward transmission to a third party;

126.4 secretive clients, in particular those with non-face to face relationship;

126.5 client or party(ies) to the transaction from suspect territories such as the NCCTs;

126.6 use of a power of attorney or trust, especially when there is no apparent reason for the client to authorise a third party to deal with assets on his behalf by creating a power of attorney or trust;

126.7 suspect personality, such as a person known or suspected to be a triad member, drug trafficker or criminal or who is introduced by a known or suspected triad member, drug trafficker or criminal;

126.8 "u-turn" transactions, where money or assets pass from one party to another and then back to the original party;

126.9 "structuring" or "smurfing", where many lower value transactions are conducted when just one, or a few, large transactions could be used.

Property transactions

127. A property transaction is an attractive way of money laundering for it can involve any stage of the money laundering process, as described in paragraph 66.

128. The use of nominee companies as registered owners of properties, in the absence of reasonable explanation, may be suspicious.

129. The provision of funds by one party to purchase property registered in the name of another person also requires explanation. The extent of information regarding the source of funds to be obtained from the client should be determined by a risk-based approach. It is not uncommon for family members to assist another family member in purchasing property. In such a situation, a simple enquiry would be sufficient. However, in any case where funds are provided by a party with no apparent relationship with the intended owner, more extensive enquiry should be made.

130. A majority of conveyancing transactions are financed by mortgage loans. Solicitors should be alerted in situations where the purchase price is paid without such financing arrangement, in particular for clients who do not appear to have the means to make such payment themselves. Enquiries must be made on the source of funding.

131. Risk assessment must be made by solicitors when cash payments in large amounts are made as criminal proceeds are usually in the form of cash.

Examples of risk areas in acting for clients

Private client work

132. Solicitors engaging in private client work will inevitably involve learning about clients' assets, which may lead to knowledge or suspicion of money laundering or terrorist financing. If solicitors become involved in the active management of or dealing with assets of clients, they may be at risk of being involved in money laundering and terrorist financing.

Administration of estate

133. Estate administration is likely to involve financial or real property transactions. During the administration, solicitors may become aware or suspicious of certain illegal dealings or terrorist financing transactions undertaken by the deceased person. As the offences under the DTRPO, OSCO and UNATMO have no limitation on the time of the underlying crime or terrorist financing act, solicitors should consider obtaining consent from the authorized officer prior to continuing with the administration of the estate.

134. Special attention should be paid to assets in foreign jurisdictions (in particular those in NCCTs) since the definition of "money laundering activities" under the Securities and Futures Ordinance (Cap. 571) covers activities which are lawful in an overseas jurisdiction but which constitute an offence if carried out in Hong Kong.

Trust arrangements

135. Similar to administration of estates, solicitors may obtain information regarding the criminal origin of trust properties. In such a situation, the solicitor should assess whether a report to an authorized officer is necessary.

Charities

136. Where a solicitor is involved in the administration of a charity, special attention should also be paid when unusually large sums of donations are received or paid out. If appropriate, an enquiry on the identity of the donor or recipient should be made.

Corporate secretarial service, bankruptcy and insolvency practice

137. Particular attention should be paid if corporate secretarial service is to be performed for the client.

138. As solicitors in bankruptcy and insolvency practice are extensively involved in the identification of assets and liabilities of the bankrupt person or insolvent company and dealing in such assets, they are susceptible to the risk of getting involved in money laundering and terrorist financing activities.

Use of solicitor's client account

139. Solicitor's client account should not be used simply for banking purpose as money launderers may use this as a way to get around the extensive anti-money laundering measures taken by financial institutions.

140. When receiving funds from clients, solicitors should be alert and should make enquiry on the source of the funds, for payments from unknown source pose significant risk of money laundering.

141. Solicitors should not establish a client account where the identity of the client or the source of funding is unknown.

ANNEXURE 5

Recognition and reporting of suspicious transactions

142. A Systemic Approach to Identifying Suspicious Transaction was recommended by the JFIU[13] It includes:-

Step One: Recognition of suspicious financial activity indicator(s);

Step Two: Ask the client appropriate question(s) to obtain information;

Step Three: Find out client's records. Review information already known to the firm when deciding whether the apparently suspicious activity is to be expected;

Step Four: Evaluate all the above information to decide if the financial activity concerned is in fact suspicious.

143. Depending on the size of a law firm, it is advisable for law firms to appoint a compliance officer who is of sufficient seniority within the firm to act as the reception point of suspicious transaction reports and to consider what appropriate actions to take following receipt of such reports.

144. Law firms and their compliance officer (if appointed) should keep written record of all suspicious transaction reports received including information and other matters leading to the making of the report and any other information which the firm and/or the compliance officer has taken into account when considering what appropriate actions to take. If it is decided that it is not necessary to report the matter to an authorized officer, the reasons for such decision should be fully documented.

145. Where a suspicious transaction is identified, it will be necessary for the law firm to consider whether in the circumstances of the transaction there is a need to file a report.

146. Suspicious transaction reports may be made to the JFIU in one of the following ways:-

146.1 by email to **jfiu@police.gov.hk**;

146.2 by fax to 2529 4013; or

146.3 by mail to Joint Financial Intelligence Unit, GPO Box, 6555 Hong Kong

Enquiries can be made on the JFIU Hotline 2866 3366 or 2860 3404.

147. Law firms should note the following points as regards the making of a report to the JFIU:

(a) No disclosure should be made to the client or any third party of any matter that may prejudice any investigation which may be conducted following such report, otherwise, the "tipping off" offence may be committed (see paragraph 44 above).

(b) If the report is made before the law firm deals with any property which is the subject of such report (e.g. the payment or receipt of money or the transfer or receipt of any property), the law firm must wait to receive the consent of the relevant authority before it actually deals with the property.

[13] Joint Financial Intelligence Unit

(c) If the report is made after the law firm deals with any property which is the subject of such report, the report must be made on its own initiative and as soon as it is reasonable (or, depending on the relevant statutory provision, as soon as it is practicable) for the firm to do so. In this case, the law firm should also be able to demonstrate when it first knew or had suspicion(s) that the property represented the proceeds of an indictable offence (or was used or intended to be used in connection therewith), and that it intended to make the report and has a reasonable excuse for any delay in making it.

ANNEXURE 6

(Repealed)

ANNEXURE 7

LIST OF FATF MEMBERS AND OBSERVERS (AS AT MARCH 2023)

FATF Members

1. Argentina
2. Australia
3. Austria
4. Belgium
5. Brazil
6. Canada
7. China
8. Denmark
9. European Commission
10. Finland
11. France
12. Germany
13. Greece
14. Gulf Co-operation Council
15. Hong Kong, China
16. Iceland
17. India
18. Ireland
19. Israel
20. Italy
21. Japan
22. Korea
23. Luxembourg
24. Malaysia
25. Mexico
26. Netherlands
27. New Zealand
28. Norway
29. Portugal
30. Russian Federation*
31. Saudi Arabia
32. Singapore
33. South Africa
34. Spain
35. Sweden
36. Switzerland
37. Turkey
38. United Kingdom
39. United States

* FATF suspended membership of the Russian Federation on 24 February 2023

FATF Observer Country

1. Indonesia

FATF Associate Members

1. Asia/Pacific Group on Money Laundering (APG) *(See also: APG website)*
2. Caribbean Financial Action Task Force (CFATF) *(See also: CFATF website)*
3. Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) *(See also: Moneyval website)*
4. Eurasian Group (EAG) *(See also: EAG website)*
5. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) *(See also: ESAAMLG website)*
6. Financial Action Task Force of Latin America (GAFILAT) (formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD)) *(See also: GAFILAT website)*
7. Inter Governmental Action Group against Money Laundering in West Africa (GIABA) *(See also: GIABA website)*
8. Middle East and North Africa Financial Action Task Force (MENAFATF) *(See also: MENAFATF website)*
9. Task Force on Money Laundering in Central Africa (GABAC) *(See also: GABAC website)*

ANNEXURE 8

BENEFICIAL OWNER

A "beneficial owner" —

(a) in relation to a corporation—

(i) means an individual who—

(A) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;

(B) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or

(C) exercises ultimate control over the management of the corporation; or

(ii) if the corporation is acting on behalf of another person, means the other person;

(b) in relation to a partnership—

(i) means an individual who—

(A) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;

(B) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or

(C) exercises ultimate control over the management of the partnership; or

(ii) if the partnership is acting on behalf of another person, means the other person;

(c) in relation to a trust, means—

(i) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;

(ii) the settlor of the trust;

(iii) the trustee of the trust

(iv) a protector or enforcer of the trust; or

(v) an individual who has ultimate control over the trust; and

(d) in relation to a person not falling within paragraph (a), (b) or (c)—

(i) means an individual who ultimately owns or controls the person; or

(ii) if the person is acting on behalf of another person, means the other person.

ANNEXURE 9

CATEGORIES OF SPECIFIED INTERMEDIARIES IN SECTION 18, DIVISION 4, PART 2, SCHEDULE 2 TO AMLO

S18(3) The specified intermediary is—

(a) any of the following persons who is able to satisfy the financial institution or the DNFBP that they have adequate procedures in place to prevent money laundering and terrorist financing—

(i) an accounting professional;

(ii) an estate agent;

(iii) a legal professional;

(iv) a TCSP licensee;

(b) a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker;

(c) a lawyer, a notary public, an auditor, a professional accountant, a trust or company service provider or a tax advisor practising in an equivalent jurisdiction, or a trust company carrying on trust business in an equivalent jurisdiction, or a person who carries on in an equivalent jurisdiction a business similar to that carried on by an estate agent, or an institution that carries on in an equivalent jurisdiction a business similar to that carried on by an intermediary financial institution, that—

(i) is required under the law of that jurisdiction to be registered or licensed or is regulated under the law of that jurisdiction;

(ii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO; and

(iii) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities or the regulatory bodies (as may be applicable); or

(d) in the case of a financial institution, an institution that—

(i) is a related foreign financial institution in relation to the financial institution; and

(ii) satisfies the conditions in subsection 18(3A).

S18(3A) The conditions are that—

(a) the related foreign financial institution is required under group policy—

(i) to have measures in place to ensure compliance with requirements similar to the requirements imposed under Schedule 2 to the AMLO; and

(ii) to implement programmes against money laundering and terrorist financing; and

(b) the related foreign financial institution is supervised for compliance with the requirements mentioned in paragraph (a) at a group level—

(i) by a relevant authority; or

(ii) by an authority in an equivalent jurisdiction that performs, in relation to the holding company or the head office of the financial institution, functions similar to those of a relevant authority under the AMLO.