Hong Kong Institute of
Certified Public Accountants
香港會計師公會

April 2015 (revised)

Anti-money Laundering Bulletin

Requirements on

Anti-Money Laundering,

Counter-Terrorist Financing

and

Related Matters

AMLB1

Anti-Money Laundering Bulletin

Contents

A. Aims and purpose

1. This purpose of this anti-money laundering bulletin ("Bulletin") is to draw members' attention to Hong Kong legislation and international developments on anti-money laundering and counter-terrorist financing ("AML/CTF"). It sets out recommended good practices, which may assist members to fulfil their ethical and legal obligations in relation to AML/CTF and to avoid inadvertent involvement in such activities. While aimed primarily at members in practice, it may also be informative and useful for members in business. This Bulletin does not constitute legal advice to members. In case of doubt, members should seek their own legal advice

2. The Bulletin replaces the original edition of July 2006. The main changes from the 2006 version are that the importance, not only of suspicious transaction reporting, but also of conducting effective due diligence on customers and record keeping, is highlighted, in line with international standards; the information in the Bulletin has been re-ordered and some of the more detailed information has been moved to the Appendix; a contents page has been added, links to websites and documents have been updated and some key links have been incorporated into the main text.

B. Introduction and background

3. "Money laundering" is defined in the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)("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."[1]

4. It covers various methods of changing the identity of the source of the proceeds of crime to disguise their illegal origin and make them appear legitimate.[2] In essence, under Hong Kong law, a person may commit an offence of money laundering if he/she carries out a transaction involving property, including money, in circumstances in which he/she knows that the property represents the proceeds of crime, or has reasonable grounds for believing that the property represents the proceeds of crime, where anyone looking at those grounds would also believe that. (See paragraph 19, below.)

5. "Terrorist financing" is the financial support of terrorism or those who encourage, plan, or engage in terrorism.[3] Terrorists or terrorist organisations require financial support in order to achieve their aims. "Terrorist financing" includes the financing of terrorist acts, and of terrorists and terrorist organisations. This generally entails the carrying out of transactions involving funds owned by terrorists, or which have been, or are intended to be, used to assist in the commission of terrorist acts. There is often a need

---

[1] AMLO, Schedule 1, Part 1.

[2] See *Anti-Money Laundering & Counter-Terrorist Financing - A Practical Guide for: Accountants, Estate Agents, Precious Metals and Precious Stones Dealers and Trust and Company Service Providers* (Narcotics Division, Security Bureau, 2009) (http://www.nd.gov.hk/pdf/moneylaundering/AML_eng_full_version.pdf, p. 11).

[3] Ibid., p. 13.

for terrorists to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

6. "Terrorist financing", under AMLO, "means -

   (a) the provision or collection, by any means, directly or indirectly, of any property

      (i) with the intention that the property be used; or
      (ii) knowing that the property will be used,

      in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);

   (b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

   (c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate."[4]

7. In the above definition, "terrorist", "terrorist act" and "terrorist associate" have the meanings given by section 2(1) of the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 ("UNATMO").

8. Money laundering and terrorist financing manipulations are similar, having to do with concealment and disguise. Money launderers will send the proceeds of crime through legal channels to conceal their criminal origin, while financiers of terrorism will transfer funds, which may be legal or illegal, to conceal the source and ultimate use, i.e., the support of terrorism.

9. The Financial Action Task Force ("FATF") is an international inter-governmental body that sets standards and promotes AML/CFT measures. It has issued the Recommendations ("Rs") as a framework to detect and prevent money laundering and terrorist financing ("ML/TF") activities. The Rs are important and are used as the basis of, or as a reference for, legislation and regulation in many jurisdictions around the world. As a member of FATF, Hong Kong is required to implement the Rs.

10. The core Rs cover suspicious transaction reporting, customer due diligence ("CDD") and record keeping, and they apply not only to financial institutions but also to specified professional services providers (referred to as "Designated Non-financial Businesses and Professions ('DNFPBs')", including accountants, in relation to specified service offerings. (See section F of the Bulletin.) Members of the Institute, therefore, should be ready to play their part in AML/CTF.

11. There is existing legislation in Hong Kong, applicable to everyone, which prescribes criminal offences for involvement in ML/TF and includes requirements on reporting suspicious transactions. Legislation prescribing CDD and record keeping requirements by financial institutions, in line with the core Rs, has also been introduced in Hong Kong. Corresponding legislation for the DNFPBs is expected to be introduced in due course.

[4] AMLO Schedule 1, Part 1.

12. Pending the introduction of legislation for DNFBPs, as member practices are bound by the Code of Ethics for Professional Accountants to conduct themselves with integrity and professionalism, and to act in the public interest, not only the interests of their clients, they may be expected to have in place adequate CDD or "know your client" procedures and arrangements for maintaining documentation, to minimise any risk of involvement in ML/TF. Therefore, to address and mitigate the legal, regulatory and reputational risks of being found to be involved in facilitating ML/TF, or not reporting known or suspected ML/TF activities, it is in member practices interests to take on board the relevant core Rs within their risk management programmes.

13. Against this background, member practices may wish to evaluate their existing procedures against the relevant Rs, and the principles and requirements on CDD and record keeping applicable to financial institutions, under AMLO.

C. Current legislation in Hong Kong

14. The main pieces of legislation in Hong Kong[5] to combat money laundering and terrorist financing activities in relation to drug trafficking, organised and serious crimes, terrorism and financial services are:

    (a) Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 ("DTROP").

    (b) Organised and Serious Crimes Ordinance, Cap. 455 ("OSCO").

    (c) UNATMO.

    (d) AMLO.

15. The following commentary on certain important provisions in the above legislation is not intended as a legal interpretation and member practices should seek legal advice where necessary.

Drug Trafficking (Recovery of Proceeds) Ordinance and Organised and Serious Crimes Ordinance

16. DTROP provides for the tracing, confiscation and recovery of the proceeds of drug trafficking and creates a criminal offence of laundering such proceeds. OSCO, key provisions of which are modelled on DTROP, extends the scope of the money laundering offences to cover the proceeds of indictable offences generally.

17. Some of the relevant provisions of DTROP and OSCO are summarised below:

Dealing in the proceeds of crime

18. Under section 25 of both DTROP and OSCO, it is a serious offence, carrying a maximum penalty, upon conviction, of 14 years' imprisonment and a fine of five million dollars, to deal with any property, knowing or having reasonable grounds to believe that it, in whole or in part, directly or indirectly, represents the proceeds of an

[5] Legislation can be accessed at the Department of Justice's bilingual laws information system (http://www.legislation.gov.hk/eng/home.htm).

indictable offence.[6] "Dealing" has quite a wide definition, including receiving or acquiring, disguising and disposing of property. (See the Appendix.)

19. As regards the interpretation of "having reasonable grounds to believe", in the recent case of *HKSAR v Pang Hung Fai*, the Court of Final Appeal ("CFA"), referencing the judgment of the Appeal Committee of the CFA, in *Seng Yuet Fong v HKSAR*[7], stated: "To convict, the jury had to find that the accused had grounds for believing; and there was the additional requirement that the grounds must be reasonable: That is, that anyone looking at those grounds objectively *would* so believe." (Emphasis added).

20. The CFA also considered that the terminology of "subjective" and "objective" tests, which had appeared in decisions following the line of authority from the case of *HKSAR v Shing Siu Ming & Others*[8], was unnecessarily complicated and liable to confuse.[9]

21. "Proceeds of an offence" has a broad definition that include payments or rewards, property derived from such payments or rewards, or any financial advantage (which could include, e.g., a cost saving). (See the Appendix.)

22. "Indictable offence" is defined in the Crimes Ordinance (Cap. 200), as "any offence other than an offence which is triable only summarily". This means that an offence that may be tried either summarily or on indictment is regarded as an indictable offence for the purposes of DTROP/ OSCO[10], and consequently the range of relevant offences is broad. The offences listed in Schedules 1 and 2 of OSCO are examples of indictable offences.

23. Various court decisions have interpreted the offence under section 25 quite widely. For example, it is unnecessary for the prosecution to prove that a specific indictable offence has been committed[11] or to specify an indictable offence in the charge[12].

24. It is a defence to a charge of dealing for a person to prove that, as required under section 25A(1):

    (a) He/she had intended to disclose knowledge or suspicion that property represented the proceeds of, was used or was intended to be used in connection with, an indictable offence, together with any matter on which that knowledge or suspicion was based, to an authorised officer, as soon as it was reasonable for him to do so; and

    (b) He/she has a reasonable excuse for his/her failure to make a disclosure.[13]

25. It should be noted that, references to an indictable offence in sections 25 and 25A of DTROP/ OSCO include conduct outside of Hong Kong that would have been an indictable offence had it taken place here.[14] Therefore, it may be an offence for a

---

[6] DTROP and OSCO, s. 25. In DTROP, s. 25 refers to the proceeds of drug trafficking.

[7] Paragraphs 52 and 70 of *HKSAR v Pang Hung Fai* [2014] HKCFA 96*; Seng Yuet Fong v HKSAR* [1999] 2 HKC 833 at 836E-F.

[8] *HKSAR v Shing Siu Ming* [1999] 2 HKC 818.

[9] Ibid., paragraphs 49-50.

[10] Section 23A, Crimes Ordinance. See also s. 14A, Criminal Procedures Ordinance (Cap. 221)

[11] *HKSAR v Li Ching* CACC 436/1997; [1997] 4 HKC 108; *HKSAR v Wong Ping Shui & Others* [2000] 1 HKC 600, which was affirmed by the Appeal Committee of the Court of Final Appeal in FAMC 1/2001.

[12] *HKSAR v Lam Hei Kit* FAMC 27/2004.

[13] DTROP and OSCO, s. 25(2).

[14] DTROP and OSCO, s. 25(4).

person to deal with criminal proceeds, under section 25(1), or fail to disclose, under section 25A(1), even if the relevant action or crime took place outside Hong Kong.

26. This provision should not be interpreted too narrowly. For example, the evasion of taxes in another jurisdiction may be an indictable offence in this context, even though the specific type of tax in question, e.g., capital gains tax, may not exist in Hong Kong. On the other hand, this does not imply that, ordinarily, a person is expected to know the law of other jurisdictions, or that a person could be in breach of the law in Hong Kong if he acted in a particular way without having such knowledge.

Reporting suspicious transactions

27. Both DTROP and OSCO have requirements, under section 25A, to report suspicious transactions, which apply to everybody in Hong Kong.

28. A person should make a disclosure to an authorised officer as soon as it is reasonable for him/her to do so, if he/she knows or suspects that any property:

(a) in whole or in part, directly or indirectly, represents the proceeds of an indictable offence[15];

(b) was used in connection with an indictable offence; or

(c) is intended to be used in connection with an indictable offence.

29. An offence of failing to make a disclosure, in accordance with section 25A, carrries a maximum penalty, upon conviction, of imprisonment for three months and a fine at level 5.[16]

30. If a person who has made the necessary disclosure does any act in contravention of section 25(1) on dealing (see above), and the disclosure relates to that act, he/she does not commit an offence, if the disclosure is made:

(a) before he/she acts, and that act is done with the consent of an authorised officer; or

(b) after he/she acts, and the disclosure is made on his/her own initiative, as soon as it is reasonable for him/her to make it.[17]

31. DTROP and OSCO make it clear that a disclosure under section 25A will not be a breach of contract, enactment, rule of conduct, or provision restricting disclosure of information. The person making the disclosure will not be liable in damages for loss arising out of the disclosure.[18]

32. Under the law, disclosures by an employee to an appropriate person according to the employer's procedures are regarded as being the same as disclosures to an authorised officer.[19]

[15] OSCO, s. 25A(1). In DTROP, s. 25A(1) refers to drug trafficking.
[16] Standard levels of fines under various ordinances are specified in Schedule 8, Criminal Procedure Ordinance.
[17] DTROP and OSCO, s. 25A(2)
[18] Ibid., s. 25A(3)
[19] Ibid., s. 25A(4)

"Tipping off"

33. A person commits an offence of “tipping off”, if, knowing or suspecting that a disclosure has been made under section 25A(1) or (4), he/she discloses to any other person any matter that is likely to prejudice an investigation that might be conducted following the original disclosure.[20] An offence of tipping off carries a maximum penalty, upon conviction, of imprisonment for three years and a fine of HK$500,000.

34. There are other provisions in DTROP and OSCO, of which members may wish to take note, regarding investigation and access to information. More information on these provisions can be found in the Appendix.

The United Nations (Anti-Terrorism Measures) Ordinance

35. UNATMO is directed primarily towards implementing Resolution 1373 of the United Nations Security Council, dated 28 September 2001, to prevent the financing of terrorist acts. Among other things, it criminalises the supply of funds and making funds, or financial services, available to terrorists or terrorist associates. It permits terrorist property to be frozen and subsequently forfeited. Some of the relevant provisions of UNATMO are summarised below:

Reporting under UNATMO

36. UNATMO requires a person to report to an authorised officer if he knows or suspects that any property is terrorist property.[21] The definition of "authorised officer", and "terrorist property", and related definitions, are contained in the Appendix.

37. Notices of the names of persons designated as terrorists or terrorist associates are published in the government gazette, under section 4 of UNATMO and regulations issued under the United Nations Sanctions Ordinance (Cap. 537). The notices reflect designations made by the United Nations Committee pursuant to UNSC Resolution 1267. UNATMO provides that it should be presumed, in the absence of contrary evidence, that a person specified in such notices is a terrorist or a terrorist associate.

38. UNATMO contains other provisions in relation to disclosure, tipping off, etc., similar to those in DTROP and OSCO:

    (a) Section 14(5) creates an offence of failing to disclose knowledge or suspicion that any property is terrorist property, pursuant to section 12(1). Like the corresponding offence under DTROP/OSCO, it carries a maximum penalty, upon conviction, of three months imprisonment and a fine at level 5.

    (b) Section 12(2) states that if a person who has made a disclosure acts in contravention of section 7 or 8[22] on funding terrorists and their associates, and the disclosure relates to that act, the person does not commit an offence if the disclosure is made:

        (i) before he/she acts, and that act is done with the consent of an authorised officer; or

[20] Ibid., s. 25A(5)
[21] Ibid., s. 12(1)
[22] UNATMO, s.7 prohibits the provision or collection of property to commit terrorist acts. Section 8 prohibits making property, etc., available to, or collecting property, etc. for, terrorists and terrorist associates.

(ii) after he/she acts, and the disclosure is made on his/her own initiative, as soon as practicable.

(c) Section 12(3) states that a disclosure will not be a breach of any contract, enactment, rule of conduct or provision restricting disclosure of information; and the person making the disclosure will not be liable in damages for losses arising out of the disclosure.

(d) Section 12(4) states that disclosures made by an employee to an appropriate person according to the employer's procedures are regarded as being the same as disclosures to an authorised officer.

(e) Section 12(5) creates a “tipping off” offence, where a person, knowing or suspecting that a disclosure has been made, discloses to any other person, any matter that is likely to prejudice any investigation that might be conducted following the original disclosure.

Investigations and access to information

39. Part 4A contains similar provisions to OSCO on investigation and access to information, including protection for legal privilege.

Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance

40. AMLO sets out CDD and record keeping requirements for financial institutions and the powers of relevant authorities to supervise compliance. It also covers regulation of money services and licensing of money service operators. As indicated above (paragraph 11), similar legislation is expected to be enacted in due course covering DNFBPs, including accountants, in line with the relevant FATF core Rs.

41. Part 2 and Schedule 2 cover the specifics of the CDD and record keeping requirements.

42. Section 7 of AMLO authorises a relevant authority (i.e., primarily the financial service regulators) to publish any guideline that it considers appropriate to provide guidance on the operation of Schedule 2. Under section 7(4), a failure by a person to comply with a guideline in published under section 7 does not, by itself, render the person liable to judicial or other proceedings, but the guideline is admissible in evidence in court proceedings under AMLO, and if any provision of the guideline appears to the court to be relevant to any question arising in the proceedings, the provision must be taken into account in determining that question.

43. Under AMLO, financial institutions may rely on CDD conducted by certain types of intermediary, including certified public accountants practising in Hong Kong, subject to specific conditions. This may be relevant where, for example, an intermediary is introducing or acting on behalf of its client. (Further information is contained in the Appendix.)

D. Recommended policies and procedures

General

44. Members should be aware of the obligations imposed by DTROP, OSCO and UNATMO. As legislation similar to AMLO is likely to be introduced for DNFPBs, in the future, AMLO may also provide a useful reference. In addition, members should take note of the core Rs applicable to accountants, discussed below and in section F.

45. In particular, members are encouraged to report suspicious transactions promptly and should note that they may commit an offence if they fail to report.[23]

46. Member practices should establish policies and procedures to comply with the existing legal requirements on AML/CFT and, more generally, to safeguard themselves against the legal and reputational risks of being found to be involved in facilitating ML/TF or not reporting known or suspected ML/TF activities, as a result of having inadequate controls in place. They should regularly monitor the effectiveness of these policies and procedures, including verification through their internal audit/ compliance function.

47. Member practices should ensure members of staff are aware of their statutory responsibilities and of steps the practice has taken to support its partners and staff to fulfil these responsibilities, including any internal consultation about and reporting of suspicious transactions. This also includes being sensitive to the risk of tipping off during their client work.

Suspicious transaction indicators

48. The types of transactions that may be used for money laundering and terrorist financing are wide-ranging. It is difficult, therefore, to specify all the transactions that might arouse suspicion.

49. Members and member practices should consider indicators of suspicious transactions, such as the nature and parties involved, including jurisdictions that insufficiently apply FATF Rs and designated terrorists published in the government gazette.

50. Particular care should be taken when, for example, companies have very complex ownership structures that do not seem to serve any legitimate purpose, or when a company is incorporated or administered in a jurisdiction designated by FATF among the Non-Cooperative Countries and Territories (More information on these countries/ territories can be found on the FATF website.)

51. According to the Joint Financial Intelligence Unit ("JFIU")[24], common indicators of suspicious activities associated with ML/TF in Hong Kong include:[25]

    (a) Large or frequent cash transactions, either deposits or withdrawals.

    (b) Suspicious activity based on transaction patterns, e.g.,

[23] DTROP and OSCO, s. 25A, and UNATMO, s. 12

[24] JFIU was established in 1989 and is run jointly by the Hong Kong Police Force and Customs & Excise Department. Its role is to receive, analyse and store suspicious transactions reports, and disseminate them to the appropriate investigative units.

[25] http://www.jfiu.gov.hk/en/str.html

(i) Accounts used as a temporary repository for funds.

(ii) A period of significantly increased activity amid relatively dormant periods.

(iii) "Structuring" or "smurfing" i.e., many lower-value transactions conducted when one, or a few, large transactions could be used. This is common in incoming remittances from countries with value-based transaction reporting requirements, e.g., frequent remittances just below AU$10,000 from Australia or US$10,000 from United States.

(iv) "U-turn" transactions, i.e., where money passes from one person or company to another and then back to the original person or company.

(v) Increased level of account activity on the first banking day after Hong Kong horse racing, normally Mondays and Thursdays, which may indicate illegal bookmaking.

(c) Involvement of one or more of the following entities, which are common in money laundering,

(i) Shelf or shell companies.

(ii) Companies registered in a known "tax haven" or "off-shore financial centre".

(iii) Company formation agent, or secretarial company, as the authorised signatory of the bank account.

(iv) Remittance agents or money changers.

(v) Casinos.

(d) Currencies, countries or nationals of countries, commonly associated with international crime, or drug trafficking, or identified as having serious deficiencies in their AML/CFT regimes.

(e) Customers who refuse, or are unwilling, to provide explanations of financial activities, or provide explanations assessed to be untrue.

(f) Activity that is unexpected of customers, considering existing knowledge about the customers and their previous financial activity. For personal accounts, relevant considerations include customers' age, occupation, residential address, general appearance, type and level of previous financial activity. For company accounts, relevant considerations include the type and level of activity.

(g) Countries, or nationals of countries, commonly associated with terrorist activities or the persons or organisations designated as terrorists or their associates.

(h) International and politically exposed persons ("PEPs"); that is, individuals who hold important positions in governments or the public sector, who may be more vulnerable to corruption and involvement in abuse of public funds.

52. Reference can also be made to:

(a) Examples of suspicious transactions in the guidelines on AML/CFT for different financial services providers in Hong Kong, issued by:

(i) Hong Kong Monetary Authority ("HKMA"), (paragraphs 7.39 to 7.44)

(ii) Office of the Commissioner of Insurance ("OCI"), (annexes 1 and 2)

(iii) Securities and Futures Commission ("SFC"), (paragraphs 7.39 to 7.40);

(iv) Commissioner of Customs and Excise ("CCE") (paragraph 7.14);

(b) Suspicious transaction indicators for accountants in the publication, *Anti-Money Laundering & Counter Terrorist Financing*, published by the Narcotics Divisions, Security Bureau, June 2009 (paragraph 4.5).

(c) Characteristics of financial transactions that may be a cause for increased scrutiny contained in Annex 1 of FATF's *Guidance for Financial Institutions in Detecting Terrorist Financing*.

(d) Relevant overseas examples, such as the general and accountancy-specific suspicious transaction indicators in *Guideline 2: Suspicious Transactions*, issued by the Financial Transactions and Reports Analysis Centre of Canada.

Disclosure of suspicious transactions

53. As indicated at paragraph 27, the statutory requirement to report suspicious transactions applies to everyone in Hong Kong. Under the law, employees may disclose their knowledge or suspicion that certain activities may be related to ML/FT to a person designated to receive such reports by their employer (sometimes referred to as an AML compliance officer). By making appropriate disclosures to the designated person, in accordance with procedures laid down by their employer, employees are regarded as having discharged their obligations under the law to report to an authorised officer (paragraphs 32 and 38(d), above).

54. Therefore, each member practice should designate a person of sufficient seniority as a compliance officer, to whom disclosures should be made internally in the first instance.

55. The compliance officer should:

(a) be responsible for making disclosures to the JFIU;

(b) keep a register of all disclosures made to him/her by employees and to the JFIU;

(c) on request, provide written acknowledgements of a disclosure made to him/her by an employee.

56. Where a member working in a member practice has knowledge or suspicion that any property:

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

(b) was used in connection with an indictable offence;

(c) is intended to be used in connection with an indictable offence; or

(d) is terrorist property,

the member should inform the compliance officer, regardless of whether the member believes a disclosure has already been made by another person, e.g., the client, to the JFIU or other authorities.

57. The compliance officer should then promptly evaluate, whether in his/her view, there are suspicious circumstances that would require a report to the JFIU. If there are, he/she should report all relevant details to the JFIU, without undue delay. He/she should co-operate with any resulting JFIU investigation. If, on the other hand, a decision is made not to report, he/she should document the reasons.

58. In relation to the section 25A of DTROP and OSCO and section 12 of UNATMO, actual suspicion on the part of the employee is required, i.e., a subjective standard of suspicion applies. It should be noted that this differs from the test of "having reasonable grounds to believe", under section 25 of DTROP/OSCO on "dealing" (paragraphs 18 -19 above).

59. According to the guideline on AML/CFT issued by the SFC, HKMA, OCI and CCE, knowledge is likely to include:

(a) actual knowledge, knowledge of circumstances that would indicate facts to a reasonable person; and

(b) knowledge of circumstances that would put a reasonable person on inquiry.[26]

60. Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence.[27] According to the guidance issued by the Consultative Committee of Accountancy Bodies in the United Kingdom, in relation to the United Kingdom legislation, having knowledge means actually knowing that something is the case.[28] This guidance also indicates that, with reference to case law, suspicion is a state of mind more definite than speculation. While it falls short of knowledge based on evidence, it must be based on some evidence, even if that evidence is tentative.[29]

61. One quite-frequently-referred-to description is: "…A suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a slight opinion, but without sufficient evidence" (Queensland Bacon PTY Ltd v Rees [1966] 115 CLR 266 at 303, per Kitto J).[30]

62. In the more recent case of Da Silva[31], the court stated: "It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."[32]

63. When reporting suspicious transactions to the JFIU, sufficient information should be

---

[26] *Guidelines on anti-money laundering and counter-terrorist financing (2012)*: SFC, HKMA , OCI and CCE (all at paras.7.8 – 7.9).
[27] Ibid.
[28] The Consultative Committee of Accounting Bodies, 2008, *Anti-money laundering guidance for the accountancy sector*, (http://www.ccab.org.uk/PDFs/CCAB%20guidance%202008-8-26.pdf, para. 2.25).
[29] Ibid., paragraph 2.26).
[30] Ibid., paragraph 2.27.
[31] Da Silva [2006] EWCA Crim 1654.
[32] Ibid.

provided, including, e.g., the following details[33]:

(a) Personal particulars of the person or company involved, e.g., name, identity card or passport number, date of birth, address, telephone number, and bank account number.

(b) Details of the suspicious transaction.

(c) The reason why the transaction is suspicious, i.e., which suspicious activity indicators are present.

(d) The explanation, if any, given by the person about the transaction.

64. To assist the disclosure of all relevant information, JFIU has provided a form on its website. A disclosure to the JFIU can be made through the e-reporting system STREAMS, email, fax, mail or telephone. Details are available on the JFIU website.[34]

65. In relation to section 25A(2) of DTROP and OSCO and section 12(2) of UNATMO, a member who has made a disclosure should, where appropriate, seek permission from the JFIU to continue to perform his/her duties in relation to the client. Where applicable, such consent should be sought through the compliance officer. If there is no immediate need for action, the JFIU should give its consent.

66. In certain circumstances, it may not be feasible to stop conducting a transaction that is known, or suspected, to be related to ML/TF, before informing the JFIU, or to do so would likely frustrate efforts to pursue the beneficiaries of a suspected ML/TF operation. Where possible, members should, nevertheless, alert the compliance officer to the situation.

67. It is not an offence where a person, prior to making a disclosure, deals with property which he/she knows, or has reasonable grounds to believe, represents the proceeds of an indictable offence, provided that a disclosure is made on his/her own initiative, as soon as reasonable after performing the act. (See paragraphs 30 and 38, above).

68. In relation to section 25A(5) of DTROP and OSCO, and section 12(5) of UNATMO, those who know or suspect that a disclosure has been made should ensure that no information is given to any person who is likely to prejudice the investigation of the disclosure, to avoid triggering an offence of “tipping-off”.

69. A person cannot be held liable for a tipping-off offence unless that person knows or suspects that a disclosure has been made, either internally or to the JFIU, or alternatively knows or suspects that the law enforcement agencies are conducting or intending to conduct an ML/TF investigation on the persons or entities concerned.

70. Therefore, unless the enquiring staff member has knowledge or suspicion of a current or impending investigation, where a member practice seeks additional information during preliminary enquiries of a prospective client, this should not give rise to a tipping-off offence. However, if the enquiries lead to a subsequent report being made, then the client must not be informed or alerted.

71. If further enquiries of a client become necessary, where it is known or suspected that a disclosure has already been made, the client must not be made aware that relevant agencies have been alerted of his/her name.

[33] http://www.jfiu.gov.hk/en/str.html#what.
[34] http://www.jfiu.gov.hk/en/str.html#how.

72. It is a defence that it was not known or suspected that the disclosure was likely to prejudice an investigation. Therefore, where a member practice communicates suspicions of ML/TF activities to a client's senior management, internal auditors, or other person responsible for monitoring, or reporting, ML/TF, the member practice should first be satisfied that:

    (a) the persons to whom it is communicating its suspicions are not implicated in the ML/TF; and

    (b) the information communicated will not be passed to others that may prejudice the investigation or proposed investigation.

73. A member practice may also communicate its suspicions to a client's regulator if this is permitted and considered appropriate. However, this is not a substitute for reporting to the JFIU.

74. A member practice may wish to terminate its relationship with a client that is being, or is likely to be, investigated. However, before terminating a relationship, a member practice should consider liaising with the JFIU, or the investigation officer, to ensure that the termination does not tip off the client, or prejudice the investigation. In more complex situations, a member practice may also wish to take legal advice as to whether the termination could be a breach of contract.

75. As indicated above (paragraphs 31 and 38(c)), in relation to 25A(3) of DTROP and OSCO and section 12(3) of UNATMO, a disclosure made to the JFIU will be not be a breach of contract, enactment, rule of conduct or provision restricting the disclosure of information. The person who made it will not be liable in damages for loss arising out of the disclosure.

76. Therefore, member practices and their employees should note that the statutory duty to make disclosures, where applicable, overrides the duty of confidentiality owed to clients. However, the protection extends only to the disclosure of knowledge or suspicion of ML/TF, and any matter on which that knowledge or suspicion is based. Disclosures should be made in good faith and based on genuine knowledge or suspicion. If in doubt, a member practice should consider seeking legal advice before making a disclosure.

77. For further information see the frequently-asked questions on suspicious transaction reporting, which forms a supplement to this Bulletin. (See: http://www.hkicpa.org.hk/file/media/section5_membership/Professional%20Representation/AMLB1%20supplement.pdf)

Customer due diligence and record keeping

78. The above recommended policies and procedures relate specifically to identifying and reporting suspicious transactions. In practice, suspicions may arise when considering acceptance of potential new clients or carrying out ongoing CDD. While AMLO covers requirements on CDD and record keeping for financial institutions, as noted above, currently the law in Hong Kong does not cover these areas for the DNFBPs included within the scope of FATF's Rs. However, as explained above (paragraph 12), member practices may be expected to, and for good risk management purposes should, take on board the relevant FATF Rs, notwithstanding the absence of legal or regulatory backing for them in Hong Kong.

79. Specifically, in relation to CDD and record keeping, member practices are recommended to take note of the FATF Rs that apply to DNFBPs, which are outlined below. It should be noted that the relevant FATF Rs refer to accountants in professional firms (paragraph 95(a), below), in particular when they are conducting the specific activities referred to in paragraph 96(a), below, and also to trust and company service providers, when they are conducing the activities referred to in paragraph 96(b), below. The statutory requirements applicable to financial institutions in Schedule 2 of AMLO also provide a useful point of reference.

80. R10 requires the following CDD measures to be applied:

(a) Identifying the customer and verifying that identity using reliable, independent sources.

(b) Identifying the beneficial owner, and taking reasonable measures to verify that identity. For legal persons and arrangements, this should include understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and transactions undertaken throughout the relationship, to ensure that the transactions are consistent with the knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.[35]

81. According to the interpretive note to R10, reliance may be placed on the results of applying the above measures, unless there is reason to doubt the veracity of the information. However, doubt may arise where, e.g., there is a suspicion of ML/TF relating to the client, or a material change in the operation of the client's account that is inconsistent with the client's business profile.[36]

82. R11 requires that all necessary records on domestic and international transactions be kept to comply swiftly with information requests from the competent authorities. Such records must permit reconstruction of individual transactions to provide evidence for prosecution of criminal activity, including the amounts and currencies.

83. It also requires that the following should be kept for, at least five years after the business relationship ends, or after the date of the occasional transaction:

(a) All records obtained through CDD measures , e.g., copies or records of official identification documents like passports, identity cards, driving licences or similar documents;

(b) account files and business correspondence, including the results of analyses undertaken, e.g., inquiries to establish the background and purpose of complex, unusual, large transactions.[37]

84. In addition to normal CDD measures, R12 requires the following enhanced measures for foreign PEPs, whether the PEP is a customer or beneficial owner:

(a) Have appropriate risk management systems to determine whether the customer

[35] For more guidance, see details in Recommendation 10 and its interpretative note.
[36] FATF interpretative note 10, para.10, p. 62.
[37] For more guidance, see details in FATF R11.

or the beneficial owner is a PEP;

(b) obtain senior management approval for establishing or continuing such business relationships;

(c) take reasonable measures to establish the source of wealth and funds; and

(d) conduct enhanced ongoing monitoring of the business relationship.

85. It also requires reasonable measures to determine whether a customer or beneficial owner is a domestic PEP, or a person who is or has been entrusted with a prominent function by an international organisation. Higher risk business relationships with such persons would require the measures in paragraphs (b), (c) and (d) to be applied. The requirements should also apply to family members or close associates of the PEPs.[38]

86. R15 requires that the ML/TF risks that may arise in the following situations be identified, assessed, managed and mitigated:

(a) The development of new products and business practices, including delivery mechanisms; and

(b) the use of new or developing technologies for both new and pre-existing products.

Adopting a risk-based approach

87. Not all client assignment/ acceptance and ongoing maintenance will carry the same level of risk and, therefore, it should not be necessary to apply the same degree of controls in each and every situation. Member practices may wish to take note of the FATF's *Guidance on the Risk-based Approach for Accountants* (in particular, section three) the purpose of which is to:

- Support the development of a common understanding of what the risk-based approach involves.
- Outline the high-level principles involved in applying the risk-based approach.
- Indicate good practice in the design and implementation of an effective risk-based approach.

88. In this context, member practices should consider conducting a risk assessment of their client base and service offering portfolio, to identify those elements that are more likely to be problematic. While this may have regard in particular to the service offerings identified by the FATF in its core Rs for accountants (paragraph 97(a) below), it should not be presumed that higher risk situatons will be limited to those service offerings identified by the FATF.

89. In practice, therefore, in applying a risk based approach, members may wish to conduct CDD on all clients and all service offerings, but to designate certain situations, including those involving these five offerings, as higher risk in relation to which extended CDD procedures may be required.

[38] For more guidance, see details in FATF R12 and interpretative note 12.

Code of Ethics for Professional Accountants

90. Members should also be aware that there are sections of the Code of Ethics for Professional Accountants that may also be relevant to the subject of this Bulletin, including:

    (a) Part B, section 270 on custody of client assets

        For example, section 270.3 states: "*As part of client and engagement acceptance procedures for services that may involve the holding of client assets, a professional accountant in public practice shall make appropriate inquiries about the source of such assets and consider legal and regulatory obligations. For example, if the assets were derived from illegal activities, such as money laundering, a threat to compliance with the fundamental principles would be created…*"

    (b) Part D, section 410 on unlawful acts or defaults by clients of members

        Section 410.76 – 410.78, for example, draws members' attention specifically to section 25 of DTROP. As noted above, relevant provisions of OSCO, including section 25, are modelled those of DTROP. However, the scope of OSCO is wider than DTROP, extending to all indictable offences, not only drug trafficking-related offences.

E. Organisations other than member practices

91. Members working in organisations other than member practices should ascertain whether their employers have procedures for making disclosures through a compliance officer. Employees that make relevant disclosures in accordance with procedures laid down by their employers are regarded as complying with the relevant laws.[39] In the absence of employer's procedures, any disclosures would need to be made direct to the JFIU.

92. Members working in the banking, insurance and securities industries are advised to familiarise themselves with AMLO and guidelines on AML/CFT issued by the HKMA, OCI and SFC, respectively.

93. Members working in trust and company service providers should be aware that this sector constitutes a separate category of DNFBPs. In this regard, the outline and explanation of key FATF Rs (see section F below) will also be relevant to members working in trust and company service providers.

F. Financial Action Task Force Recommendations and their implications

94. The FATF Rs originally applied only to financial institutions, but subsequently key Rs were extended to DNFBPs. Some of the more important Rs applicable to DNFBPs are summarised below:

95. Firstly, DNFBPs include:

[39] DTROP and OSCO, s.25A(4) and UNATMO, s.12(4).

(a) lawyers, notaries, other independent legal professionals and accountants. This refers to sole practitioners, partners or employed professionals within professional firms. It is not intended to cover "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures;[40]

(b) trust and company service providers. This refers to all persons or businesses that are not covered elsewhere under the Rs, and which, as a business, provide any of the following services to third parties:

(i) acting as a formation agent of legal persons;

(ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(iii) providing a registered office; business address or accommodation, correspondence or administrative address for a company, partnership or any other legal person or arrangement;

(iv) acting as (or arranging for another person to act as) a trustee of an express trust, or performing the equivalent function for another form of legal arrangement; or

(v) acting as (or arranging for another person to act as) a nominee shareholder for another person.[41]

Customer due diligence and record keeping – Rs10, 11, 12, 15, and 17

96. The CDD and record keeping requirements are in Rs10, 11, 12, 15, and 17. They apply to specific categories of DNFBPs in the following circumstances:

(a) Under R22(d), to lawyers, notaries, other independent legal professionals and accountants, when assisting clients in the following activities:

(i) buying and selling of real estate;

(ii) managing of client money, securities or other assets;

(iii) management of bank, savings or securities accounts;

(iv) organisation of contributions for the creation, operation or management of companies;

(v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(b) under R22(e), to trust and company service providers, when assisting clients in the following activities:

[40] FATF, 2012, *The FATF Recommendations* (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf, glossary, p. 113).
[41] *FATF Recommendations* (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf, glossary, p. 113-114).

(i) acting as a formation agent of legal persons;

(ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

(iv) acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

(v) acting as (or arranging for another person to act as) a nominee shareholder for another person.

97. R10, which requires the various CDD measures to be implemented; R11, which relates to record keeping; R12, which requires enhanced CDD to be applied to foreign PEPs, whether the PEP is a customer or beneficial owner, and R15, which covers AML/ CFT in relation to new products and business practices and the use of new or developing technologies, are all outlined above (paragraphs 78 - 86).

98. R17 allows authorities to permit financial institutions to rely on third parties to perform the CDD measures in R10(a) to (c), or to introduce business, provided that the following criteria are met:

(a) A financial institution relying on a third party should immediately obtain the information for the CDD measures in R10(a) to (c).

(b) The financial institution should satisfy itself that copies of relevant documentation for the CDD requirements will be available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored, and has measures in place to comply with the CDD and record keeping requirements in Rs10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should consider the risk level of the base country.[42]

99. As indicated above (paragraph 43 and the Appendix), AMLO has incorporated similar provisions to allow financial institutions in Hong Kong to rely on CDD carried out by certain third parties.

Suspicious transaction reporting – Rs18 to 21

100. Rs 18 to 21 apply to all DNFBPs, subject to the following qualifications:

(a) Under R23(a), lawyers, notaries, other independent legal professionals and accountants should report suspicious transactions when assisting clients in a financial transaction relating to the activities in R22(d). Authorities are also

[42] For more, see FATF R17 and interpretive note 17.

strongly encouraged by FATF to extend the reporting requirement to other professional activities of accountants, including auditing;

(b) under R23(c), trust and company service providers should report suspicious transactions when assisting clients in a transaction relating to the activities in R22(e).

101. R18 requires AML/CFT programmes to be implemented. Group entities should implement group-wide programmes, including policies and procedures for sharing information on AML/CFT.[43]

102. R19 requires enhanced CDD measures for business relationships and transactions with natural and legal persons, and financial institutions, from higher-risk countries, where this is called for by the FATF.[44]

103. R20 requires that, if it is suspected or there are reasonable grounds to suspect, that funds are the proceeds of a criminal activity, or are related to terrorist financing, by law, the suspicion should be promptly reported to the financial intelligence unit.[45]

104. R21 requires that, by law, those who report suspicions:

(a) in good faith, should be protected from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by legislative, regulatory or administrative provision, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) should be prohibited from disclosing (tipping off) the fact that a suspicious transaction report or related information is being filed with the financial intelligence unit.[46]

105. As noted above (paragraph 53) the relevant legislative provisions in Hong Kong (i.e., DTROP, OSCO and UNATMO) go further than R21 and apply to everyone and are not limited to specific type of transactions.

106. Interpretative notes to R23 qualify the requirement to report suspicions, as follows:

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.

107. However, while accountants may be regarded in some jurisdictions as “acting as independent legal professionals” in certain situations, it should be noted that this has no clear application in the case of Hong Kong. Therefore, it would not be advisable for members rely upon this concept when considering whether or not to make a suspicious transaction report.

[43] For more, see FATF R18 and interpretive note 18.
[44] For more, see FATF R19 and interpretative note 19.
[45] For more, see FATF R20 and interpretative note 20. R20 has already been implemented in Hong Kong laws, through section 25A of DTROP/OSCO, section 12 of the UNATMO, and AMLO.
[46] For more, see FATF R21. R21 is already provided for under DTROP/OSCO and UNATMO.

Appendix

Relevant provisions of DTROP, OSCO, UNATMO and AMLO

A. Dealing in the proceeds of crime under DTROP and OSCO

1. "Dealing" in relation to property includes:

   (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 to 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).[47]

2. "Proceeds of an offence" covers:

   (a) any payments or other rewards received by a person at any time in connection with the commission of that offence;

   (b) any property derived or realised, directly or indirectly, by him from any of the payments or other rewards; and

   (c) any pecuniary advantage obtained in connection with the commission of that offence.[48]

3. This means that "proceeds of an offence" are not limited to actual profits or gains, but could be a "pecuniary advantage", such as a cost saving.

4. "Authorised officer" means:

   a. any police officer;

   b. any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); and

   c. any other person authorised in writing by the Secretary for Justice for the purposes of this Ordinance.[49]

B. Definitions under UNATMO

5. "Authorised officer" means:

[47] DTROP/ OSCO, s. 2.
[48] DTROP, s. 4 (refers to proceeds of drug trafficking) and OSCO, s. 2.
[49] Ibid., s. 2.

(a) a police officer;

(b) a member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342);

(c) a member of the Immigration Service established by section 3 of the Immigration Service Ordinance (Cap. 311); or

(b) an officer of the Independent Commission Against Corruption established by section 3 of the Independent Commission Against Corruption Ordinance (Cap. 204).[50]

6. “Terrorist property” means:

(a) the property of a terrorist or terrorist associate; or

(b) any other property consisting of funds that:

(i) is intended to be used to finance or otherwise assist the commission of a terrorist act; or

(ii) was used to finance or otherwise assist the commission of a terrorist act.[51]

7. “Terrorist” means a person who commits, or attempts to commit, a terrorist act, or participates in, or facilitates the commission of, a terrorist act.[52]

8. “Terrorist associate” means an entity owned or controlled, directly or indirectly, by a terrorist.[53]

9. "Terrorist act” refers to the use, or threat, of action, where this is intended to:

(a) cause serious violence against a person;

(b) cause serious damage to property;

(c) endanger a person’s life, other than that of the person committing the action;

(d) create serious risk to the health or safety of the public or a section of the public;

(e) seriously interfere with or seriously disrupt an electronic system; or

(f) seriously interfere with or seriously disrupt an essential service, facility or system, whether public or private; and

(g) and the use or threat is:

(i) intended to compel the government, or to intimidate the public, or a section of the public; and

(ii) made for the purpose of advancing a political, religious or ideological cause.

[50] UNATMO, s. 2.
[51] Ibid.
[52] Ibid.
[53] Ibid.

(Paragraphs (d), (e) and (f) do not include the use or threat of action in the course of any advocacy, protest, dissent or industrial action.)[54]

C. *Investigations and access to information under DTROP and OSCO*

10. For drug trafficking investigations under DTROP, a court can order a person who appears to possess or control material, or material of a particular description, to produce it to an authorised officer, or give the officer access to it. The order has effect, notwithstanding any secrecy obligation or other restriction imposed by statute or otherwise. It will not apply to items subject to legal privilege.[55]

11. A court has the power to issue a warrant allowing an authorised officer to enter specified premises to search them, and to seize and retain materials, other than items subject to legal privilege.[56] The officer may, for example, photograph or copy materials produced, to which access is given, or seized.[57]

12. The concept of legal privilege is relevant to section 25A of OSCO. In *Pang Yiu Hung v. Commissioner of Police*[58], Hartmann J. says (at paras.119-120):

"*In my judgment, on a plain reading, it is patent that the legislature intended all persons, including legal practitioners, to be subject to the obligations imposed by s.25A of OSCO…*

But while in a general sense, I believe it is patent on a plain reading of s.25A that the legislature intended both solicitors and barristers to be subject to s.25A, they, in particular, are exempted from the obligations imposed by the section, if, in order to fulfil those obligations, a breach of legal professional privilege would be required…."

13. "Items subject to legal privilege" means:

(a) communications between a professional legal adviser and his client, or any person representing his client, made in connection with the giving of legal advice to the client;

(b) communications between a professional legal adviser and his client, or any person representing his client, or between such an adviser, his client, or any such representative and any other person, made in connection with, or in contemplation of, legal proceedings and for the purposes of such proceedings; and

(c) items enclosed with, or referred to, in such communications, and made:

(i) in connection with the giving of legal advice; or

(ii) in connection with, or in contemplation of, legal proceedings and for the purposes of such proceedings,

when they are in the possession of a person who is entitled to possess them. However, any communications or items held with the intention of furthering a criminal purpose are excluded.[59]

---

[54] Ibid.
[55] DTROP, s. 20.
[56] Ibid., s. 21.
[57] Ibid., s. 22.
[58] *Pang Yiu Hung v. Commissioner of Police* (HCAL133/2002, 2.12.02).
[59] DTROP, s. 22 and OSCO, s. 2.

14. The above could, for example, include communications between:

(a) a legal adviser and an accountant representing the legal adviser's client, made in connection with the giving of legal advice to the client.

(b) a legal adviser and an accountant representing the legal adviser's client; or between a legal adviser, his client, or an accountant representing his client, and any other person; made in connection with, or in contemplation of, legal proceedings and for the purposes for such proceedings.

15. At common law, legal privilege does not cover communications made in order to obtain advice for a fraudulent or criminal purpose. Nor will it apply to communications between a client and lawyer for purposes unconnected with the obtaining of legal advice.

16. Under DTROP, it is an offence for:

(a) a person to hinder or obstruct an authorised officer in the execution of a search warrant[60].

(b) Where:

(i) an order to make material available, under section 20, has been made, or applied for and not refused; or

(ii) a search warrant to search under section 21 has been issued,

for a person, who knows or suspects that an investigation is taking place, to make any disclosure that is likely to prejudice the investigation.[61]

17. There are similar provisions in the OSCO, as follows:

(a) Section 3, on the requirement to furnish information, or produce material, in compliance with a court order. It is an offence if:

(i) a person fails to comply with the section without reasonable excuse;

(ii) a person purporting to comply, makes a statement that he knows to be materially false or misleading, or recklessly makes a statement this is materially false or misleading.

(b) Section 4, on orders to make material available.

(c) Section 5, on the authority for searches.

(d) Section 7, on the offence of prejudicing an investigation. It is an offence, where an order under section 3 or 4 has been made, or applied for and not refused, or a warrant under section 5 has been issued, for a person who knows or suspects that an investigation is taking place:

(i) without lawful authority or reasonable excuse, to make any disclosure intending to prejudice the investigation; or

[60] DTROP, s. 21.
[61] Ibid., s. 24.

(ii) falsify, conceal, destroy, or dispose of any material; or permit such to happen:

- knowing or suspecting that the material is likely to be relevant to the investigation; and

- intending to conceal the facts disclosed by the material from the investigation.

D. Reliance on intermediaries for customer due diligence under AMLO

18. Division 4, Part 2 of Schedule 2 allows CDD measures to be performed by intermediaries. A financial institution may rely on an intermediary to conduct the CDD, if the intermediary consents in writing and the financial institution is satisfied that the intermediary will, without delay, provide a copy of any record obtained by the intermediary during the CDD.[62] However, the financial institution remains liable for a failure to conduct CDD measures.[63]

19. The intermediary is:

(a) any of the following persons, who are able to satisfy the financial institution that they have adequate procedures in place to prevent money laundering and terrorist financing:

(i) a solicitor practising in Hong Kong;

(ii) a certified public accountant practising in Hong Kong;

(iii) a current member of The Hong Kong Institute of Chartered Secretaries practising in Hong Kong;

(iv) a trust company registered under Part VIII of the Trustee Ordinance (Cap 29) carrying on trust business in Hong Kong;

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

(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 an institution that carries on in an equivalent jurisdiction a business similar to that carried on by a financial institution mentioned in paragraph (b), 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 this Schedule 2; 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.

[62] AMLO, Schedule 2, Part 2, Division 4, s. 18(1).
[63] Ibid., s. 18(2).

Bibliography, References and Websites[64]

I) Financial Action Task Force

Financial Action Task Force ("FATF": http://www.fatf-gafi.org/. Information available on this site includes the following:

- *FATF International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations (and interpretative notes)* (February 2012) *http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html*

- *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* (February 2013): http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfissuesnewmechanismtostrengthenmoneylaunderingandterroristfinancingcompliance.html

- *Guidance on the Risk-Based Approach for Accountants* (June 2008): http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfguidanceontheris k-basedapproachforaccountants.html

II) Hong Kong sources

(a) Hong Kong Institute of CPAs, *Frequently Asked Question on Suspicious Transaction Reporting*, supplement to the Bulletin: http://www.hkicpa.org.hk/file/media/section5_membership/Professional%20Representation/AMLB1%20supplement.pdf

(b) Narcotics Division, Security Bureau, *Anti-Money Laundering & Counter Terrorist Financing* (June 2009): http://www.nd.gov.hk/pdf/moneylaundering/AML_eng_full_version.pdf

(c) Joint Financial Intelligence Unit: http://www.jfiu.gov.hk

(d) Hong Kong Monetary Authority, *Guideline on Anti-Money Laundering and Counter-Terrorist Financing Supplement thereto (revised July 2012)*: http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf

(e) Office of the Commissioner of Insurance, *Guideline on Anti-Money Laundering and Counter-Terrorist Financing*: http://www.oci.gov.hk/download/appendixc.pdf

(f) SFC: *Guideline on Anti-Money Laundering and Counter-Terrorist Financing*: http://en-rules.sfc.hk/en/display/display_main.html?rbid=3527&element_id=3705

(g) Securities and Futures Commission ("SFC"): Background information on Anti-Money Laundering and Counter-Terrorist Financing: http://www.sfc.hk/web/EN/rule-book/anti-money-laundering-and-counter-terrorist-financing/

[64] N.B. Website links are correct at the time of going to press and will be checked from time to time. If, at any time, members find difficulty in accessing any of the specific links above, we recommend searching for the relevant document through the home page of the relevant organisation.

(h) Hong Kong Government Gazette: http://www.gld.gov.hk/egazette/

(i) Hong Kong judgements and legal references: http://www.judiciary.gov.hk/

(j) Laws of Hong Kong at:
http://www.doj.gov.hk/eng/laws/ (English version)
http://www.doj.gov.hk/chi/laws/ (Chinese version)

(k) Law Society of Hong Kong, guidelines:
http://www.fjt2.net/gate/gb/www.hklawsoc.org.hk/pub_e/professionalguide/volume2/default.asp?cap=24.17

Other AML information: http://www.hklawsoc.org.hk/pub_e/aml/default.asp

(l) Hong Kong Institute of Chartered Secretaries, guidelines:
http://www.hkics.org.hk/media/publication/attachent/2141_AML%20Guidelines.pdf

III) International and overseas sources

a. Consultative Committee of Accountancy Bodies ("CCAB") *Anti-Money Laundering Guidance for the Accountancy Sector*:
http://www.ccab.org.uk/documents/20140217%20FINAL%202008%20CCAB%20guidance%20amended%202014-2-17pdf.pdf

b. Institute of Chartered Accountants in England and Wales ("ICAEW"), *Anti-Money Laundering Guidance for Accountants* (on-line version of the CCAB guidance (see above)):
http://www.icaew.com/en/members/regulations-standards-and-guidance/practice-management/anti-money-laundering-guidance

Other ICAEW information on AML:
http://www.icaew.com/en/products/accountancy-markets-and-ethics/~/link.aspx?_id=c777bbd2a4db4094b7ff93e2b97173f2&_z=z

c. Institute of Singapore Chartered Accountants, *Anti-Money Laundering* and *Countering the Financing of Terrorism – Requirements and Guidelines for Professional Accountants in Singapore*: http://download.isca.org.sg/tech/EP%20200.pdf

d. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), *Guideline 2: Suspicious Transactions*:
http://www.fintrac.gc.ca/publications/guide/Guide2/2-eng.asp (December 2010)

e. UK Law Society: http://www.lawsociety.org.uk/advice/anti-money-laundering/

f. International Money Laundering Information Network: https://www.imolin.org/

g. United Nations ("UN"): http://www.un.org

h. UN Security Council Sanctions Committees:
http://www.un.org/sc/committees/index.shtml