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

July 2006

Anti-money Laundering Bulletin

Requirements on

Anti-money Laundering,

Anti-terrorist Financing

and

Related Matters

AMLB1 (formerly LB1)

HONG KONG INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS
LEGAL BULLETIN

Requirements on Anti-money Laundering, Anti-terrorist Financing and Related Matters

This Legal Bulletin supersedes Technical Bulletin 13 "Drug Trafficking (Recovery of Proceeds) Ordinance 1989" issued by the Institute in August 1990. It draws members' attention to relevant provisions of the law in Hong Kong aimed at countering money laundering and terrorist financing activities, as well as international developments in this area. This Legal Bulletin does not constitute legal advice to members. In case of doubt, members should seek their own legal advice.

I. BACKGROUND

1. The term "money laundering" includes a wide range of activities and processes involving the proceeds of serious crime, which are often intended to alter the identity of the source of the proceeds in a manner that disguises their illegal origin. In essence, under Hong Kong law, any transaction involving "dealing" with the proceeds of an indictable offence (see paragraphs 26 and 27 below) is money laundering and a person may commit an offence of money laundering if he carries out a transaction involving property, including money, in circumstances in which a reasonable person would have believed that the property was the proceeds of serious crime.

2. Terrorists or terrorist organisations require financial support in order to achieve their aims. The term "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 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[1].

3. Guidelines on the prevention of money laundering and terrorist financing have been issued by the financial regulators in Hong Kong and these may provide some further background information, including examples of suspicious indicators of money laundering and terrorist financing activities that authorised institutions, insurance institutions and licensed traders may encounter on a day-to-day basis. These include the following:

    - *Guideline on Prevention of Money Laundering* issued by the Hong Kong Monetary Authority and the Supplement thereto ("HKMA Guideline");

[1] *Consultation Conclusions on the Proposed Revised Prevention of Money Laundering and Terrorist Financing Guidance Note* issued by the Securities and Futures Commission ("SFC Guidance Note") paragraphs 2.1.2 – 2.1.3.

- *Guidance Note on Prevention of Money Laundering and Terrorist Financing* issued by the Office of the Commissioner of Insurance ("OCI"), and;

- *Consultation Conclusions on the Proposed Revised Prevention of Money Laundering and Terrorist Financing Guidance Note* issued by the Securities and Futures Commission ("SFC Guidance Note")).

International Initiatives - Financial Action Task Force on Money Laundering

4. The Financial Action Task Force on Money Laundering ("FATF") is an international inter-government organisation, which sets standards and develops and promotes policies to combat money laundering and terrorist financing. It was established in 1989, in an effort to thwart attempts by criminals to launder the proceeds of criminal activities through the financial system. In November 1990, Hong Kong was invited to participate as an observer in FATF, and has, since December 1990, attended FATF meetings and played an active role in its deliberations. Hong Kong was admitted as a full member in March 1991 and, as a member, is obliged to implement its recommendations.

5. In 1990, the FATF published a series of recommended measures for dealing with money laundering, known as *The Forty Recommendations* ("40Rs"), which covered the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation against money laundering. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing when it promulgated *Eight Special Recommendations on Terrorist Financing* ("SRs"). A ninth SR in was issued in October 2004.

6. In June 2003, FATF issued a revised version of the 40Rs. The revised 40Rs extend some of the anti-money laundering (AML) measures, which were originally applied only to financial businesses, including banks and "non-bank" financial operations, such as remittance agents, to designated non-financial businesses and professions ("DNFBPs"), including accountants and lawyers, when they are undertaking certain specific activities (see the Supplement in Part IV below). Recommendation IV of the 9SRs is also relevant to DNFBPs.

7. The recommendations and guidance issued by the FATF set out a basic framework to detect, prevent and suppress money laundering and terrorist financing activities. As a member of FATF, Hong Kong is required to implement FATF recommendations although, as yet, legislation to implement the revised 40Rs in full has still to be introduced into the Legislative Council. Pending the enactment of the necessary legislation in Hong Kong, Supplement in Part IV of this Legal Bulletin outlines the broad implications of the revised 40Rs for accountants.

8. The FATF has also published guidance, such as *Guidance for Financial Institutions in Detecting Terrorist Financing* (24 April 2002) and a paper on international best practices for combating the abuse of non-profit organisations in October 2002, which was included in the booklet, *FATF: International Best Practices to Prevent the Misuse of Non-Profit Organisations for the Financing of Terrorism* released by the Security Bureau (Narcotics Division) of the Hong Kong SAR Government in February 2003. It also issues reports on methods

and trends in money laundering, referred to as "typologies", the most recent of which, *Trade Based Money Laundering*, was published in June 2006.

II. CURRENT ANTI-MONEY LAUNDERING/ANTI-TERRORIST FINANCING LEGISLATION IN HONG KONG

9. Legislation has been enacted in Hong Kong to address the problems associated with money laundering and terrorist financing activities in the areas of drug trafficking, organised and serious crimes, and terrorism. The main pieces of legislation are the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP"), Organised and Serious Crimes Ordinance ("OSCO") and United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO")[2].

DTROP (Cap. 405)
OSCO (Cap. 455)
UNATMO (Cap. 575)

10. DTROP came into force on 1 December 1989. It provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds.

11. OSCO, which was modelled on DTROP, was brought into operation in December 1994. It extended the scope of the money laundering offences to cover the proceeds of indictable offences generally.

12. Amendments to DTROP and OSCO, which came into effect on 1 September 1995, tightened the money laundering provisions in the two ordinances and introduced requirements in relation to reporting suspicious transactions. There is now a clear statutory obligation to disclose knowledge or suspicion of money laundering transactions. The relevant provisions apply to all persons, and not only to financial institutions and professionals.

13. Some of the main provisions of DTROP and OSCO that are relevant to members are summarised below. For reference, the maximum penalties for offences under the relevant provisions are indicated in the text. It should be emphasised that the following commentary is not intended as a legal interpretation of the legislation and legal advice should be sought where necessary.

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

Investigations and access to information

14. In the context of investigations into drug trafficking under DTROP, a court can order that a person who appears to be in possession or control of particular material or material of a particular description must produce it to an authorised officer or give an authorised officer access to it. Such an order has effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by statute or otherwise, although it will not apply to items subject to legal privilege. The definition of "authorised officer" under section 2 of the DTROP and OSCO is reproduced in Appendix 1, Part A.

DTROP, sections 20-22 and 2

[2] The Laws of Hong Kong can be accessed on the internet at: http://www.doj.gov.hk/eng/laws/ (English version) or http://www.doj.gov.hk/chi/laws/ (Chinese version).

15. A court has the power to issue a search warrant allowing an authorised officer to enter specified premises to perform a search and to seize and retain any material, other than items subject to legal privilege. An authorised officer may, for example, photograph or copy any material produced or to which access is given or which is seized.

16. "Items subject to legal privilege" includes, broadly:

    (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 or 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.

17. This could, therefore, include communications between a legal adviser and, for example, an accountant who is representing the legal adviser's client, made in connection with the giving of legal advice to the client; or communications between a legal adviser and an accountant representing his[3] client, or between a legal adviser or 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 of such proceedings.

18. Items subject to legal privilege may also include items enclosed with, or referred to in, the privileged communications, and which are in connection with the giving of legal advice or in connection with legal proceedings, when they are in the possession of a person who is entitled to possess them. Any communication or item held with the intention of furthering a criminal purpose is not covered.

19. Members may wish to note that, 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.

20. A person who hinders or obstructs an authorised officer in the execution of a search warrant granted commits an offence. [*Maximum penalty: Conviction upon indictment - a fine of $250,000 and imprisonment for 2 years.*] DTROP, section 21

21. In relation to the sections above, members should be aware that any person who knows or suspects that an investigation is taking place and makes any disclosure that is likely to prejudice the investigation, commits the offence of prejudicing an investigation. Disclosure to a client, who may be the subject of an investigation, therefore, could render a member liable. [*Maximum penalty: Conviction, upon indictment - a fine of $500,000 and imprisonment for 3 years.*] DTROP, section 24

[3] In this bulletin, the use of the masculine form also denotes the feminine form.

22. There are similar, although not identical, provisions in the OSCO and members should take note of these. See for example section 3 of OSCO, which relates to furnishing information or producing material in compliance with a court order.

OSCO, section 3

23. A person who without reasonable excuse fails to comply with a requirement imposed under section 3 of OSCO commits an offence. [*Maximum penalty: A fine at level 6 (currently $100,000)*[4] *and imprisonment for one year*.] A person purporting to comply, who makes a statement that he knows to be materially false or misleading, or who recklessly makes such a statement, commits an offence. [*Maximum penalty: Conviction upon indictment - a fine of HK$500,000 and imprisonment for 3 years.*]

24. Searches are dealt with under section 5 of the OSCO and the offence of prejudicing an investigation is contained in section 7. Where an order to furnish information or material, or to make material available, has been made, or applied for and not refused, or a search warrant has been obtained, a person commits an offence if, knowing or suspecting that an investigation is taking place, he:

OSCO, sections 5 and 7 (see also sections 3 and 4)

(a) without lawful authority or reasonable excuse makes any disclosure intending to prejudice the investigation; or

(b) falsifies, conceals, disposes of any material, or permits such to happen –

(i) knowing or suspecting that the material is likely to be relevant to the investigation; and

(ii) intending to conceal the facts disclosed by the material from persons conducting the investigation.

[Maximum Penalty: Conviction upon indictment - a fine and imprisonment for 7 years.]

<u>Principal money-laundering and related offences under DTROP and OSCO</u>

(As sections 25 and 25A of DTROP and OSCO are, in most respects, identical, hereinafter, in this part of the Legal Bulletin, it should be assumed that references to section and subsection numbers refer to both DTROP and OSCO, unless otherwise indicated and, similarly, references to an indictable offence also include references to drug trafficking, unless otherwise indicated)

Dealing in the proceeds of crime

25. Section 25 creates an offence of dealing 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 indictable offence.

Section 25(1)

26. "Dealing" in relation to property includes: (a) receiving or acquiring the property; (b) concealing or disguising the property (whether by concealing or disguising

Sections 2 and 25(3)

[4] The relevant monetary amounts of the different levels of fines can be found at Schedule 8 of the Criminal Procedure Ordinance (Cap. 221).

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). *[Maximum penalty: 14 years' imprisonment and a fine of $5 million.]*

27. "Indictable offence" is defined in the Crimes Ordinance (Cap.200, section 23A) as being "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. (See also section 14A of the Criminal Procedures Ordinance (Cap.221)).

28. Various court decisions have made it clear that the offence under section 25 is to be interpreted quite widely. There is no need, for example, to prove that a specific indictable offence has been committed[5] and it is not necessary to specify an indictable offence in the charge[6].

29. As regards the test for determining "having reasonable grounds to believe", under section 25, this involves both subjective and objective elements. It requires proof that (i) there were grounds that a common sense, right-thinking person would consider were sufficient to lead a person to believe that the property was linked to a serious offence, and (ii) that these grounds were known to the defendant[7]. This means that a person would commit an offence if he dealt with property, without knowing or believing that property represented the proceeds of an indictable offence, if he had reasonable grounds for knowing or believing that it did so.

30. It is a defence for a person to prove that he intended to disclose such knowledge, suspicion or matter on which that knowledge or suspicion is based, to an authorised officer as soon as it was reasonable for him to do so, and has a reasonable excuse for his failure to make a disclosure.

Sections 25(2), 25A(2)

31. There is a statutory duty for a person, who knows or suspects that any property (a) in whole or in part, directly or indirectly, represents the proceeds of an indictable offence; (b) was used in connection with an indictable offence; or (c) is intended to be used in connection with an indictable offence, to make a disclosure to an authorised officer as soon as it is reasonable for him to do so. It is an offence for a person to fail to make such disclosure. *[Maximum penalty: A fine at level 5 (currently $50,000) and 3 months' imprisonment.]*

Section 25A(1)

32. As regards item (a) in paragraph 31 above, "proceeds of an (indictable) offence" is defined quite widely in OSCO as:

OSCO, section 2

[5] *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).

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

[7] *HKSAR v Shing Siu Ming & Others* CACC 415/1997; [1997] 2 HKC 818; *Seng Yuet Fong v HKSAR* FAMC 26/1998; [1999] 2 HKC 833.

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

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

(iii) any pecuniary advantage obtained in connection with the commission of that offence.

33. A corresponding definition of "a person's proceeds of drug trafficking" can be found in DTROP. DTROP, section 4

34. Examples of indictable offences, referred to in DTROP/OSCO, include the offences listed in Schedules 1 and 2 of OSCO. It should be noted that section 25(4) of OSCO provides that references to an indictable offence in sections 25 and 25A of OSCO include a reference to conduct that would have constituted an indictable offence if it had occurred in Hong Kong. Section 25(4)

35. That is to say, it may be an offence under section 25(1) of OSCO for a person to deal with the proceeds of crime, or fail to make any disclosure as required by section 25A(1) of OSCO, even if the principal crime was not committed in Hong Kong, provided that the conduct involved would also constitute an indictable offence in Hong Kong if the conduct had occurred in Hong Kong. This should not be interpreted too narrowly. For example, the evasion of taxes in another jurisdiction may constitute an "indictable offence" for the purpose of sections 25(1) and 25A(1) of OSCO, even though the specific tax in question (e.g., capital gains tax) may not apply in Hong Kong. This does not imply that, ordinarily, a person is expected to have knowledge of the laws of other jurisdictions, including their tax laws, or would fall foul of the law if he acted in a particular way, in the absence of such knowledge.

36. It should be noted, from the definition in paragraph 32 above, that the "proceeds of an offence" are not limited to actual profits or gains. The definition extends to "any pecuniary advantage", which could, for example, include a cost saving.

Reporting suspicious transactions

37. Under section 25A, a person who knows or suspects that any property wholly or partly, directly or indirectly, represents any person's proceeds of an indictable offence, or was, or is, intended to be, used in connection with, an indictable offence, must, as soon as it is reasonable for him to do so, disclose that knowledge or suspicion and any matter on which it is based to an authorised officer. Failure to do so is an offence. [*Maximum penalty: A fine at level 5 and imprisonment for 3 months.*]

38. If a person who has made the necessary disclosures does any act in contravention of section 25(1) (on dealing) and the disclosure relates to that act, he does not commit an offence if the disclosure: Section 25A(2)

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

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

39. A disclosure will not be treated as a breach of contract, any enactment, rule of conduct or other provision restricting disclosure of information and will not render the person making the disclosure liable in damages for any loss arising out of the disclosure.

Section 25A(3)

40. DTROP/OSCO extends the provisions of section 25A to disclosures made by an employee to an appropriate person, in accordance with the procedures established by his employer for the making of such disclosures, in the same way as they apply to disclosures to an authorised officer. In other words, to the employee, making a disclosure to the designated person is sufficient to meet the requirements of the legislation. This provides protection to employees of member practices against the risk of prosecution where they have reported knowledge or suspicion of money laundering transactions to a person designated for the purpose by their employers.

Section 25A(4)

Tipping off

41. A person commits a "tipping off" offence if, knowing or suspecting that a disclosure has been made under section 25A(1) or (4), he discloses to any other person any matter that is likely to prejudice an investigation which might be conducted following the first-mentioned disclosure. [*Maximum penalty: A fine of $500,000 and imprisonment for 3 years.*]

Section 25A

42. The concept of legal privilege is relevant to section 25A of OSCO. Members may wish to note the judgment of Hartmann J. in *Pang Yiu Hung v. Commissioner of Police* (HCAL133/2002, 2.12.02) in which he said (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…."*

(The definition of "items subject to legal privilege" in OSCO is very similar to that in DTROP; see paragraph 16 above.)

OSCO, section 2
DTROP, section 22

The United Nations (Anti-Terrorism Measures) Ordinance

43. UNATMO was enacted in July 2002 and a substantive part of the law came into operation on 23 August 2002. The legislation is principally directed towards implementing decisions contained in Resolution 1373 dated 28 September 2001

of the United Nations Security Council ("UNSC") aimed at preventing the financing of terrorist acts.

44. UNATMO, among other things, 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.

45. Some of the main provisions of UNATMO that are relevant to members are summarised below. It should be emphasised that the following commentary is not intended as a legal interpretation of the legislation and legal advice should be sought where necessary.

Investigations and access to information

46. The United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004, which was passed in July 2004, introduced a new part on investigations (Part 4A) into UNATMO. This contains similar provisions to OSCO, including protection for legal privilege.

UNATMO, section 2(5)

Reporting under UNATMO

47. UNATMO requires a person to report to an authorised officer if he knows or suspects that any property is terrorist property. Failure to make a disclosure under this section constitutes an offence. *[Maximum penalty: A fine of HK$50,000 and imprisonment for 3 months.]* (The definition of "authorised officer" appears in section 2 of UNATMO (see Appendix 1, Part B). It will be noted that there are some differences between this definition and those in DTROP/OSCO.)

UNATMO, sections 12(1) and 14(5)

48. If a person who has made a disclosure does any act in contravention of section 7 or 8 of UNATMO (on the supply of funds or making funds or financial services available to terrorists and their associates) before or after such disclosure, and the disclosure relates to that act, the person does not commit an offence if the disclosure is made:

Section 12(2)

(a) before he does that act and he does that act with the consent of the authorised officer; or

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

49. A disclosure made under UNATMO will not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rules of conduct or other provision. The person making the disclosure will not be 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.

Section 12(3)

50. The provisions of section 12 are extended to disclosures made by an employee to an appropriate person in accordance with the procedures established by his employer for the making of such disclosures in the same way as they apply to disclosures to an authorised officer. As with OSCO/DTROP (see paragraph 40

Section 12(4)

above), therefore, to an employee, making a disclosure to the designated person is sufficient to meet the requirements of the legislation. This provides protection to employees against the risk of prosecution where they have reported knowledge or suspicion that any property is terrorist property.

51. A person commits a "tipping off" offence if, knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the first-mentioned disclosure. [*Maximum penalty: Conviction upon indictment – a fine and imprisonment for 3 years.*] Section 12(5)

52. The term "terrorist property" means: Section 2

(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.

53. "Funds" includes funds mentioned in Schedule 1 to UNATMO. It covers cash, cheques, deposits with financial institutions or other entities, balances on accounts, securities and debt instruments (including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, debenture stock and derivatives contracts), interest, dividends or other income on, or value accruing from, or generated by, property, documents evidencing an interest in funds or financial resources, etc.

54. "Terrorist" means a person that commits, or attempts to commit, a terrorist act or that participates in or facilitates the commission of a terrorist act. "Terrorist associate" means an entity owned or controlled, directly or indirectly, by a terrorist. The term "terrorist act" refers to the use or threat of action where the action is intended to: Section 2

(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

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.

However, in the case of paragraphs (d), (e) and (f) above, a "terrorist act" does not include the use or threat of action in the course of any advocacy, protest, dissent or industrial action.

55. A list of terrorist or terrorist associate names is published in the Government Gazette (the e-version of which can be accessed on the government website (see the Bibliography)), from time to time, pursuant to section 4 of UNATMO and section 10 of the United Nations Sanctions (Afghanistan) Regulation (Cap. 537K) (issued under the United Nations Sanctions Ordinance (Cap. 537)). The published list reflects designations made by the United Nations Committee that were established pursuant to UNSC Resolution 1267. UNATMO provides that it shall be presumed, in the absence of evidence to the contrary, that a person specified in such a list is a terrorist or a terrorist associate, as the case may be.

III. RECOMMENDED POLICIES AND PROCEDURES IN RELATION TO THE REPORTING OF MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITIES

General

56. Members should take note of the relevant sections of the three ordinances and be aware of the obligations imposed by DTROP, OSCO and UNATMO. Members are encouraged to co-operate with the law enforcement agencies by providing prompt reports of suspicious transactions and should note that they may commit an offence if they fail to report relevant information. Members should report suspicious transactions to their firm's or company's compliance officer (see paragraphs 60 and 85 below) or, where there is no compliance officer, to the JFIU, even if they do not know precisely what the underlying criminal activity may be.

Member Practices

57. Member practices are advised to establish appropriate policies and procedures to enable them to comply with the relevant legislative requirements, in particular the requirements relating to the reporting of money laundering and terrorist financing. Member practices should monitor the effectiveness of those policies and practices and ensure that their staff are aware of their responsibilities.

DTROP/ OSCO, section 25A UNATMO, section 12

58. Where appropriate, member practices should ensure that their internal audit/compliance function includes verifying, on a reasonably regular basis, adherence to policies and procedures that the practice has established to ensure compliance with the relevant requirements against money laundering and terrorist financing.

59. The aim of the recommended procedures below is to assist members and member practices in complying with the reporting requirements with respect to money laundering activities under DTROP and OSCO, and with respect to terrorist financing activities under UNATMO (collectively referred to as "the Provisions"). The recommended procedures below represent good practice, while not constituting legal advice to members. In case of doubt, member practices are advised to seek their own legal advice.

Identifying and reporting suspicious transactions

60. Each member practice should appoint a person of sufficient seniority designated as a compliance officer to whom disclosures should be made internally in the first instance. The compliance officer should be responsible for making disclosures to the Joint Financial Intelligence Unit ("JFIU", which is a unit based at the headquarters of the Hong Kong Police Force ("HKPF") and run jointly by the HKPF and the Customs & Excise Department) in accordance with the Provisions.

61. A compliance officer should keep a register of all disclosures made to him internally by employees and those made to the JFIU under the Provisions. A compliance officer should, on request, provide written acknowledgements of a disclosure made to him by an employee.

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

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

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

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

    (iv) 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 another authority. In turn, the compliance officer should as soon as practicable make any necessary disclosures to the JFIU.

63. Members may wish to note for reference that guidance issued in March 2004 by the Consultative Committee of Accountancy Bodies in the United Kingdom ("UK"), in relation to the corresponding legislative requirements in the UK, suggests that knowledge may include, for example: (i) actual knowledge; (ii) shutting one's mind to the obvious; (iii) deliberately refraining from making enquiries, the content of which one might not care to have; (iv) knowledge of circumstances which would indicate the facts to an honest and reasonable person; (v) knowledge of circumstances which would put an honest and reasonable person on enquiry and failing to make the reasonable inquiries

which such a person would have made[8]. As regards suspicion, case law and other sources indicate that suspicion is more than speculation but less than proof or knowledge. Suspicion is personal and subjective but will generally be built upon some objective foundation[9]. In relation to the disclosure requirements in Hong Kong (s.25A, OSCO/DTROP and s.12, UNATMO), generally actual suspicion on the part of the employee is required (i.e. a subjective standard of suspicion applies).

64. When a disclosure has been made to a compliance officer, the compliance officer should promptly evaluate whether, in his view, there are suspicious circumstances that would warrant a report being made to the JFIU. If there are, the compliance officer should then make any necessary disclosures to the JFIU without undue delay, ensuring that all relevant details are provided in the report. He should co-operate with the JFIU for the purpose of investigation. If a decision is made not to report a particular, apparently suspicious, transaction to the JFIU, the reasons for this should be properly documented by the compliance officer.

Suspicious transaction indicators

65. The types of transactions that may be used by a money launderer and terrorist are virtually unlimited, and it is difficult to definitively specify which transactions might constitute a suspicious transaction. Suspicion may arise, for example, where a transaction is for a purpose inconsistent with a client's known business or personal activities, or with the normal business for that type of client.

66. If, within a member practice, a suspicion begins to form that certain transactions relate to money laundering or terrorist financing, the member practice should be conscious of the risk of tipping off and handle the client due diligence process with particular care. If in doubt, the member practice should liaise with the JFIU. Member practices should ensure that their employees are aware of and sensitive to these issues when they conduct client due diligence.

67. Particular care should be taken when, for example, a corporation has an overly complex ownership structure that does not seem to serve any legitimate purpose, or when a corporation is incorporated/administered in jurisdictions designated by the FATF as the Non-Cooperative Countries and Territories (NCCTs)[10]. More information on the NCCT initiative and the current list of NCCTs can be found on the FATF website (see the Bibliography).

68. In examining terrorist-related financial activity, FATF experts have concluded that terrorists and their support organisations generally use the same methods as criminal groups to launder funds[11]. According to the JFIU (for the JFIU website, see the Bibliography), indicators of suspicious activities that are most commonly associated with money laundering or terrorist financing in Hong Kong include the following[12]:

---

[8] Institute of Chartered Accountants in England and Wales, TECH 12/04 and Handbook Statement 1.304 (paragraph 6.1)

[9] Ibid., paragraph 6.2

[10] SFC Guidance Note, *paragraph 6.2.7*

[11] FATF *Guidance for Financial Institutions in Detecting Terrorist Financing* (paragraph 15)

[12] JFIU website, under "*A Systematic Approach to Identifying Suspicious Transactions*"

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

(ii) Suspicious activities based on transaction patterns, such as:

- Accounts used as a temporary repository for funds.
- A period of significantly increased activity amid relatively dormant periods.
- "Structuring" or "smurfing", that is, many lower value transactions conducted when one, or a few, large transactions could be used, seen particularly in incoming remittances from countries with value-based transaction reporting requirements, e.g., frequent remittances of just below AUS$10,000 from Australia, or US$10,000 from USA.
- "U-turn" transactions, that is, money passes from one person or company to another and then back to the original person or company.
- Increased level of account activity on the first banking day after Hong Kong horse racing, indicating illegal bookmaking.

(iii) Involvement of one or more of the following entities, which are commonly involved in money laundering:

- Shelf or shell companies.
- Companies registered in a known "tax haven" or "off-shore financial centre".
- Company formation agents, or secretarial companies, as the authorised signatory of the bank account.
- Remittance agencies or money changers.
- Casinos.

(iv) Currencies, countries or nationals of countries, commonly associated with international crime or drug trafficking, or identified as having serious deficiencies in their anti-money laundering regimes, for example, NCCTs, as identified by the FATF.

(v) Clients that refuse, or are unwilling, to provide an explanation of financial activities, or which provide an explanation assessed to be untrue.

(vi) Activity that is not commensurate with that expected from a client, considering the information already known about the client and the client's previous financial activity. (For individual clients, consider the client's age, occupation, residential address, general appearance, type and level of previous financial activities. For corporate clients, consider type and level of activity).

(vii) Countries or nationals of countries, commonly associated with terrorist activities, or the persons or organisations designated as terrorists or their associates. The latest consolidated list pursuant to the UNSC Resolutions 1267 (1999), 1333 (2000), 1390 (2002) and 1455 (2003) can be found on the United Nations' website (see the Bibliography).

(viii) Politically Exposed Persons ("PEPs"), that is, individuals who hold important positions in governments or the public sector. It has been alleged that some PEPs in some overseas countries are involved in corruption and abuse of public funds.

69. Members and member practices should take the above indicators of suspicious activities into account, together with other relevant information, including lists of designated terrorists published in the Government Gazette (see paragraph 55 above), as well as the nature of the transaction itself and the parties involved in the transaction.

70. Reference can also be made to the examples of suspicious transactions contained in Appendix C(ii) to the SFC Guidance Note, Annex 5 to the HKMA Guideline, and the characteristics of financial transactions that may be a cause for increased scrutiny as contained in Annex 1 to the FATF's *Guidance for Financial Institutions in Detecting Terrorist Financing*.

71. Other useful references on suspicious transaction activities may be found in overseas sources (e.g., information issued by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), whose *Guideline 2: Suspicious Transactions* lists general and accountancy-specific suspicious transaction indicators (see the Bibliography).

Disclosure of suspicious transactions

72. A disclosure of suspicious transactions to the JFIU should include, e.g., the following details[13]:

- Personal particulars (e.g., name, identity card or passport number, date of birth, address, telephone number, bank account number) of the person(s) or company involved in the suspicious transaction.

- Details of the suspicious financial activities.

- The reason why the transaction is suspicious – which suspicious activity indicators are present.

- The explanation, if any, given by the person about the transaction.

To assist the disclosure of all relevant information, proformas have been made available by various bodies at the JFIU website[14]. For reference, a copy of the general form provided by the HKPF is reproduced at Appendix 2.

[13] JFIU website under *What to include in a Suspicious Transaction Report*.
[14] JFIU website under *What to Report*.

A disclosure to the JFIU can be made by mail, addressed to the Joint Financial Intelligence Unit, GPO Box 6555, Hong Kong Post Office, Hong Kong, or by email (see the Bibliography).

73. A member who has made a disclosure under the Provisions should, where appropriate, seek permission from the JFIU through the compliance officer to continue to perform his duties in relation to the client. If there is no immediate need for action, consent will usually be given by the JFIU under the provisions of section 25A(2) of DTROP/OSCO or section 12(2) of UNATMO.

74. In certain circumstances, it may not be possible to refrain from carrying out a transaction that is known or suspected to be related to money laundering or terrorist financing before informing the JFIU, or to do so would be very likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. Where possible, a member should nevertheless alert the compliance officer to the situation.

75. Under section 25A(2) of DTROP/OSCO and section 12 of UNATMO a person who, prior to making a disclosure, deals with property which he knows, or where there are reasonable grounds to suspect, that the property represents the proceeds of an indictable offence, does not commit an offence provided that a disclosure is made (i) after performing the act; (ii) on his own initiative; and (iii) as soon as it is reasonable for him to make the disclosure (see paragraphs 38 and 48 above.

DTROP/OSCO, section 25A(2) UNATMO, section 12

76. 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, thus triggering the operation of the "tipping-off" offence provisions in section 25A(5) of DTROP/OSCO and in section 12(5) of UNATMO (see paragraphs 41 and 51 above).

DTROP/OSCO, section 25A(5) UNATMO, section 12(5)

77. A tipping-off offence cannot arise unless the person concerned 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 carrying out or intending to carry out a money laundering or terrorist financing investigation on the persons or the companies involved in the suspicious transaction. Therefore, where a member practice seeks additional information while conducting preliminary enquiries of a prospective client, this should not give rise to a tipping-off offence, unless the enquirer has knowledge or suspicion of a current or impending investigation. However, if the enquiries lead to a subsequent report being made, then the client must not be informed or alerted.

78. It is a defence in this context that it was not known or suspected that the disclosure was likely to prejudice an investigation. Where a member practice communicates suspicions of money laundering or terrorist financing activities to a client's senior management, internal auditors, or other person responsible for monitoring or reporting money laundering and terrorist financing, therefore, the member practice should first be satisfied that (i) that the persons to whom it is communicating its suspicions are not in any way implicated in the money laundering or terrorist financing, and (ii) that the information that it is communicating will not be passed to others, so as to risk any investigation or proposed investigation being prejudiced. A member practice may also

communicate its suspicions to a client's regulator if this is considered appropriate.

79. Where it is known or suspected that a disclosure has already been made and it becomes necessary to make further enquiries of a client, great care should be taken to ensure that the client does not become aware that its name has been brought to the attention of the relevant agencies.

80. A member practice may wish to terminate its relationship with a client that is (or is likely to become) subject to an investigation. However, it must avoid tipping-off the client when doing so.

81. Before terminating a relationship in these circumstances, 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 any other way. In more complex situations, member practices may also wish to take legal advice as to whether termination could have breach of contract implications.

82. As indicated above, a disclosure made to the JFIU under the Provisions, (i) will 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; and (ii) will not render the person who made it 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.

83. Therefore, member practices and their employees should note that the statutory duty to make disclosures under the Provisions, where applicable, overrides their duty of confidentiality owed to clients. However, the protection extends only to the disclosure of knowledge or suspicion of money laundering or terrorist financing, and any matter on which that knowledge or suspicion is based. Disclosures should, therefore, be made in good faith, and not for vexatious or frivolous reasons, and be based on genuine knowledge or suspicion. If in doubt, a member practice should consider seeking legal advice before making a disclosure.

84. Member practices should take reasonable steps to ensure that all employees concerned with client work of any description are familiar with these recommended procedures and are made aware that it is a criminal offence to fail to comply with the statutory disclosure requirements.

Organisations Other than Member Practices

85. Members working in organisations other than member practices should ascertain as to whether their employers have procedures in place for making disclosures through compliance officers. In cases where such procedures are in place, members making disclosures in accordance with their respective organisation's usual procedures for the making of such disclosures are regarded as having complied with the relevant disclosure requirements. In the absence of such procedures, it would be necessary for members to make disclosures direct to the JFIU.

86. Members working in the banking, insurance and securities industries are advised to familiarise themselves with the HKMA Guideline and the Supplement thereto, the *Guidance Note on Prevention of Money Laundering and Terrorist Financing* issued by the OCI, and the SFC Guidance Note, as appropriate (see paragraph 3 above).

Code of Ethics for Professional Accountants

87. Members should also bear in mind relevant provisions of the *Code of Ethics for Professional Accountants* when considering matters covered in this Bulletin (e.g., Part B, section 270 (*Custody of Client Assets*) and Part D, sections 410 (*Unlawful Acts or Defaults by Clients of Members*) and 411 (*Unlawful Acts or Defaults by or on Behalf of a Member's Employer*)).

IV. SUPPLEMENT

Implications of FATF's Revised 40 Recommendations

88. As indicated in paragraph 6 above, the FATF's revised 40Rs extend some of the anti-money laundering framework to DNFBPs, which include accountants and lawyers, when they are performing certain functions. As an FATF member jurisdiction, Hong Kong is expected to implement these changes. As yet the full legal and regulatory framework has not been put in place and so the most of the new FATF requirements currently do not have the force of law in Hong Kong. However, DTROP and OSCO have already implemented the requirements on suspicious transaction reporting in Hong Kong (see, e.g., paragraphs 105-107 below).

89. Nevertheless, member practices should consider the need to prepare for the changes that will take place. For reference, therefore, this Bulletin outlines the key requirements of the FATF regime as it affects practising accountants.

90. Members may refer to the following documents, all of which can be accessed on the FATF's website:

- *The Forty Recommendations*
- *Interpretative Notes to the Forty Recommendations*
- *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations ("Methodology")*

91. A definition of DNFBPs appears in the glossary of the *Forty Recommendations*. Insofar as it relates to accountants, it refers to "sole practitioners, partners or employed professionals within professional firms" (see Appendix 3). The definition further clarifies: "It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering".

92. The core FATF recommendations relate to customer due diligence, record keeping and suspicious transaction reporting. These apply to (i) accountants, amongst others, when they prepare for or carry out transactions for a client concerning the activities specified in FATF R12(d), and (ii) trust and company service providers[15], when they prepare for or carry out transactions for a client concerning the activities referred to in FATF R12(e). Recommendations 5, 6, 8-11 and 13-15 of the revised 40Rs set out the basic requirements relating to client due diligence measures (which include, e.g., identifying and verifying the identity of the client and the beneficial owner), record-keeping and reporting suspicious transactions.

(i) The activities specified in R12(d) are as follows:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies; or
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(ii) The activities to which R12(e) refers are as follows[16]:

- acting as a formation agent of legal persons;
- 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;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust; or
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

[15] Defined in the glossary as all persons or businesses that are not covered elsewhere under the 40Rs and which, as a business, provide to third parties any of the services referred to in the definition (see paragraph 92 below).

[16] The activities are listed in the glossary of *The Forty Recommendations* and R12(e) cross-refers to them.

Customer due diligence - FATF Recommendations 5, 6, 8 and 9

93. When performing elements (a) and (b) of the client due diligence measures (see of the 40Rs), i.e., (a) identifying the client and verifying that client's identity using reliable, independent source documents, data or information; and (b) identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner to ascertain who the beneficial owner is, and in the case of legal persons and arrangements, to understand the ownership and control structure of the client, the measures to be taken are to:

    (i) verify that any person purporting to act on behalf of the client is so authorised, and identify and verify the identity of that person;

    (ii) identify the client and verify its identity by, e.g., obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the client's name, the names of trustees (for trusts), legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement;

    (iii) identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons by, e.g., identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement. Where the client or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company;

    (iv) obtain information on the purpose and intended nature of the business relationship; and

    (v) conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the known background of the client, its business and risk profile, including, where necessary, the source of funds.

94. The relevant information may be obtained from a public register, from the client or from other reliable sources.

95. A member practice would be entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead a practice to have such doubts could be where there is a suspicion of money laundering in relation to that client, or where there is a material change in the way that the client's account is operated, which is not consistent with the client's business profile.

Record keeping – FATF Recommendations 10-11

96. FATF R10 provides that all necessary records on transactions, both domestic and international, should be kept for at least five years following completion of the transaction, to enable compliance with information requests from the competent authorities.

97. Such records should be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

98. Records on identification data obtained through the carrying out of the client due diligence measures (e.g., copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence should also be kept for at least five years after the business relationship is ended.

99. Under R12(d) of the revised 40Rs, the client due diligence and record-keeping requirements, set out in Rs 5, 6, and 8 to 11, apply to DNFBPs such as accountants when they prepare for or carry out transactions for their client concerning the activities listed in paragraph 92(i) above.

100. Under R12(e), trust and company service providers are subject to the client due diligence and record-keeping requirements, set out in Rs 5, 6, and 8 to 11, when they prepare for or carry out transactions for a client concerning the activities listed in paragraph 92(ii) above.

Suspicious transaction reporting – Recommendations 13-15 (and 21)

101. According to R16(a), the reporting requirements under, e.g., R13 apply to accountants when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in R12(d) (see paragraph 92(i) above). Recommendation 16(a) also states that countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

102. According to R16(c), the reporting requirements under, e.g., R13 apply to trust and company service providers when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in R12(e) (see paragraph 92(ii) above).

103. Recommendation 13 provides that, where it is suspected that, or where there are reasonable grounds to suspect that, funds are the proceeds of a criminal activity, or are related to terrorist financing, an obligation to report such suspicions arises.

104. The *Methodology* explains the difference between the tests of “suspecting” and “having reasonable grounds to suspect” as follows: “The requirement to report when the individual ‘suspects’ is a subjective test of suspicion, i.e., the person actually suspects a transaction involved a criminal activity. A requirement to report when there are ‘reasonable grounds to suspect’ is an objective test of suspicion and can be satisfied if the circumstances surrounding the transaction

would lead a reasonable person to suspect that the transaction involved a criminal activity" (C.f. S.25A of OSCO/DTROP and s.12 of UNATMO, see paragraph 63 above.). The *Methodology* goes on to say that this "requirement implies that [jurisdictions] may choose either of the two alternatives, but need not have both".

105. Thus, R13 has already been implemented in law in Hong Kong through section 25A of the DTROP/OSCO and section 12 of the UNATMO (see paragraphs 37 and 47, respectively, above).

106. Recommendation 14 provides that those who report their suspicions in good faith should be:

    (i) protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any 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;

    (ii) prohibited by law from disclosing the fact that a suspicious transaction report is being made.

107. These additional provisions of R14 are also already provided for under DTROP/OSCO and UNATMO (regarding (i), see paragraphs 39 and 49, respectively, above and, as regards (ii), see paragraphs 41 and 51 above, which refer to the offence of "tipping off").

108. The requirement to report suspicions is modified by the following qualification appearing under R16:

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

109. It should be noted that, while accountants may be regarded in some jurisdictions as "acting as independent legal professionals" in certain situations, this has no clear application in the case of Hong Kong and it would not be advisable to rely upon it as, for example, a means of protecting client confidentiality. As indicated in paragraph 83 above, under Hong Kong law, the requirement to report suspicious transactions would, generally, override any professional duty of client confidentiality.

110. More information on the work of and publications issued by the FATF can be found on the FATF website.

Hong Kong Institute of Certified Public Accountants
July 2006

Bibliography, References and Websites[17]

Consultative Committee of Accountancy Bodies / Institute of Chartered Accountants in England and Wales, *Anti-Money Laundering (Proceeds of Crime and Terrorism) Second Interim Guidance for Accountants TECH 12/04* (March 2004) at: http://www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_62604 (also issued as Handbook Statement 1.304).

Financial Action Task Force on Money Laundering at: http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html.

Information available on this site includes the following:

- *The Forty Recommendations (20 June 2003) and associated Interpretative Notes*
- *Nine Special Recommendations on Terrorist Financing (22 October 2004) and associated Interpretative Notes*
- *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (27 February 2004)*
- *Guidance for Financial Institutions in Detecting Terrorist Financing (April 2002).*

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

Government Gazette at: http://www.gld.gov.hk/egazette/.

Hong Kong Monetary Authority, *Guideline on Prevention of Money Laundering (December 2000), and Supplement thereto (June 2004)* at: http://www.info.gov.hk/hkma/eng/guide/index.htm (Guideline) http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a3.pdf (Supplement).

Joint Financial Intelligence Unit at: http://www.jfiu.gov.hk.

Judgements and legal references at: http://www.judiciary.gov.hk/en/index/index.htm .

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

Office of the Commissioner of Insurance, *Guidance Note on Prevention of Money Laundering and Terrorist Financing (July 2005)* at: http://www.oci.gov.hk/download/gn3jul05.pdf.

Securities and Futures Commission, *Consultation Conclusions on the Proposed Revised Prevention of Money Laundering and Terrorist Financing Guidance Note (October 2005)* at: http://www.sfc.hk/sfc/doc/EN/speeches/public/consult/05/money_laundering_conclusions_0510_eng.pdf.

United Nations, *Consolidated list pursuant to UNSC Resolutions* at: http://www.un.org/docs/sc/committees/1267/1267ListEng.htm.

[17] 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 organisation concerned.

APPENDIX 1

Definition of "Authorised Officer"

Part A

Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) and Organised and Serious Crimes Ordinance (Cap. 455) (section 2)

"authorized 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."

Part B

United Nations (Anti-Terrorrism) Measures Ordinance (Cap. 575) (section 2)

"authorized officer" (獲授權人員) means-

(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

(d) an officer of the Independent Commission Against Corruption established by section 3 of the Independent Commission Against Corruption Ordinance (Cap. 204).

APPENDIX 2

HKP Suspicious Transaction Reporting Proforma
For Reports Made Under S. 25A of the DTROP & OSCO

I.	Source Name of person making report : …… …… Name of company making report : ……..…… Address of company making report : …….. …… Tel No. : ..…….. Fax No. :…….. Date of Report …… Reporting Company Ref No. ……...
II.	Details of the Suspicious Activity (Provide details of the transaction(s) and the reason(s) why you consider it/them to be suspicious).
III.	Suspicious Activity Indicators Observed (List the suspicious activity indicators which are present)
IV.	Explanation Given by the Subject of the Report (What was the subject's explanation for carrying out the suspicious transaction?)
V.	Details of The Subject Name : ……..…… M/F : ……..…. DOB : …… HK ID or other identification doc. & type : …….. Address : …….. ……Tel No. : ……... Bank Account (name of bank and a/c No.) : ……..…… Occupation : …… Company : ……..….. Company Address : …… ……
VI.	Details of Other Entities Involved In The Suspicious Activity

APPENDIX 3

"Designated Non-Financial Businesses and Professions" (extracted from the *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*)

"Designated non-financial businesses and professions" means:

a) Casinos (which also includes internet casinos).

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- 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;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.