STATEMENT OF AUDITING PRACTICE

SAP 1

Guidance to Auditors on Money Laundering and Terrorism Financing

This Statement of Auditing Practice was approved by the Council of the Institute of Singapore Chartered Accountants (formerly known as Institute of Certified Public Accountants of Singapore) in September 1998.

SAP 19 supersedes the SAP of the same title in June 2004. No substantive changes have been made to the original approved text and all cross references have been updated, as appropriate.

This revised SAP 19 supersedes SAP 19 “The Auditor’s Role and Responsibilities in relation to the Prevention, Detection and Reporting of Money Laundering” in November 2006.

SAP 19 was renumbered to SAP 1 for greater clarity and consistency in February 2013.

Contents

	paragraphs
Preamble	1-6
Introduction	7-14
Responsibilities of Management	15-16
General Responsibilities of Auditors	17-22
Criminal Offences	23-28
Guidance on measures auditors need to establish	29-30
Know-Your-Customer ("KYC")	31-37
Conduct of the audit	
Planning and performing the audit	38-39
Fraud	40-41
Laws and regulations	42-44
Additional considerations for audits of entities in the financial sector	45-46
Reporting and Tipping-off	47-49
Confidentiality, statutory immunity and legal privilege	50-53
Knowledge and Suspicion	54-63
Procedures when possible money laundering or terrorism financing is discovered	64-69
The auditor's report on financial statements	70-71
Records Keeping	72-74
Training	75-79

Appendix A: Description of Money Laundering and Terrorism Financing

Appendix B: Summary of Basic Criminal Offences Under Anti-Money Laundering Legislation

Appendix C: Summary of Basic Criminal Offences Under Terrorism-Financing Legislation

Appendix D: Summary of Basic Criminal Offences Under the Penal Code

Appendix E: Factors Indicating an Increased Risk of Money Laundering

Appendix F: Indicative Report Content

STATEMENT OF AUDITING PRACTICE

SAP 1

Guidance to Auditors on Money Laundering and Terrorism Financing

PREAMBLE

1. When the Drug Trafficking (Confiscation of Benefits) Act ("DTA") was first enacted, drug trafficking was viewed as the primary source of funds for money laundering. The original Statement of Auditing Practice ("SAP") 19 of September 1998 was issued to provide guidance to auditors in Singapore concerning money laundering and its relationship with their responsibilities when auditing and reporting on financial statements.

2. Since then, there has been evidence that significant money laundering is not restricted to only proceeds from drug-related activities but also from other serious crimes. As a result, our laws were subsequently amended to extend anti-money laundering ("AML") provisions beyond drug trafficking to cover other serious crimes. Threats of terrorism and the need to effectively fight terrorism has also resulted in the enactment of new anti-terrorism financing ("ATF") legislation to criminalise terrorism financing.

3. Furthermore, as Singapore is a member of the Financial Action Task Force on Money Laundering ("FATF"), an international task force established to combat money laundering and terrorism financing on a global scale, it is obliged to comply with and implement the "Forty Recommendations" on AML and "Nine Special Recommendations" on ATF issued by the FATF.

4. The revised AML and new ATF legislation provide a framework for discouraging money laundering and terrorism financing by, for example, establishing criminal sanctions for such activities and requiring the reporting of suspicious transactions to the authorities.

5. These legislation have implications on the responsibilities of auditors, including the risk of criminal liability on auditors for non-compliance.

6. The purpose of this revised SAP is to provide auditors in Singapore with updated information about our current AML and ATF legislation, and guidance on compliance with those legislation. This SAP also provides guidance to auditors as to their responsibilities on auditing and reporting on financial statements.

Introduction

7. Money is "laundered" to conceal criminal activity associated with it, including the crimes that generate the money, for example, drug trafficking, fraud and criminal breach of trust. The term ”money laundering” covers any activity by which the apparent source and ownership of money representing the proceeds of crime are changed so that the money appears to have been obtained legitimately. Terrorism financing refers to the direct or indirect act of providing or collecting property for terrorist acts, providing property and services for terrorist purposes, using or possessing property for terrorist purposes, and dealing with property of terrorists. A brief description of money laundering and terrorism financing is set out in Appendix A.

8. Whilst the AML and ATF legislation applies to auditors in the same way as it does to other individuals and organisations, it does not place obligations directly on auditors in their capacity as such. Nevertheless, the nature of the work undertaken by auditors may bring them into contact with terrorism financing activities or circumstances where proceeds of criminal activity is or may be laundered. Consequently, whilst in the normal course of auditing practice the matters referred to in this SAP may rarely become a matter of concern, the consequences of inaction or unwise action when terrorism financing or the laundering of criminal proceeds is or may be occurring could be serious. Auditors need to be aware of the appropriate actions to take.

9. This SAP takes into consideration the following primary AML and ATF legislation in Singapore:

   (a) primary legislation setting out criminal offences directly in relation to money laundering which apply to any person, regardless of the capacity in which he or she is acting. These offences are set out in the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act, Cap. 65A (“CDSA”). The CDSA also imposes a duty on a person, who in the course of his or her professional duties comes to know or suspect that any property represents the proceeds of drug trafficking or criminal conduct, to report the knowledge or suspicion to the relevant authorities. A summary of the key provisions is set out in Appendix B;

   (b) primary legislation setting out criminal offences directly in relation to terrorism financing which apply to any person, regardless of the capacity in which he or she is acting. These are set out in the Terrorism (Suppression of Financing) Act, Cap. 325 (“TSFA”). The TSFA also imposes a duty on a person who has possession, custody or control of terrorist property, or information regarding a transaction in terrorist property, to report such information to the relevant authorities. Furthermore, a person who has information which can prevent the commission of a terrorism financing offence, or assist in the apprehension, prosecution or conviction of a person for a terrorism financing offence, is required to immediately inform the relevant authorities. A summary of the key provisions is set out in Appendix C; and

   (c) primary legislation setting out criminal offences indirectly in relation to money laundering which apply to any person, regardless of the capacity in which he or she is acting. These offences are set out in sections 107, 108 and 108A of the Penal Code, Cap. 224. A summary of the key provisions is set out in Appendix D.

10. The extent to which AML and ATF legislation affects the auditor's work differs between two broad categories of audit:

    (a) *audits of certain Monetary Authority of Singapore ("MAS") regulated entities:* certain entities in this category, such as banks, merchant banks and holders of Capital Markets Services licence, are required to comply with specific secondary legislation establishing additional obligations on them. These secondary legislation comprise Regulations, Notices and Guidelines issued by the MAS which set out certain prohibited businesses and require these institutions to implement and maintain certain procedures to forestall or prevent money laundering and terrorism financing. These entities are also normally expected by the regulators to adopt best practices guidelines issued by their respective industry associations, if any.

    In addition to reporting on their financial statements, their auditors are required to report to the MAS on matters of significance that come to their attention in the course of their work, including non-compliance with legislation, departures from its requirements and suspicions that the directors and management of such entities are implicated in money laundering. Therefore, their auditors should also be aware of key provisions contained in those secondary legislation and best practices guidelines issued by industry associations; and

    (b) *audits of other types of entity:* in general, auditors of other types of entity are required only to take appropriate steps in response to factors encountered in the course of their work which lead them to suspect that money laundering or terrorism financing is taking place. This is discussed later in this SAP.

11. This SAP gives guidance concerning the effects of AML and ATF legislation on the work undertaken in relation to reporting on the financial statements of entities in each of the two categories above, including the auditor's statutory reporting duties.

12. However, this SAP:

    (a) does not address issues further to those set out in this SAP which may arise when auditing the financial statements of financial sector entities, such as further reports to a regulator or other authority which may be required in relation to these entities' arrangements to prevent and detect money laundering and terrorism financing, their compliance with legislation and regulation; or their systems of controls more generally;

    (b) does not constitute legal advice, which an auditor should consider obtaining to address specific situations that the auditor faces, such as if the auditor wishes to adopt legal interpretations that are different from those set out in this SAP; and

    (c) should not be regarded as guidance on foreign legislation. Therefore, auditors who perform services outside Singapore should consider the need to familiarise themselves with the foreign AML and ATF legislation in order to mitigate the risk of committing offences in that foreign country.

13. Members, including accounting firms, accounting corporations and accounting limited liability partnerships, may also provide other services, such as secretarial, insolvency and tax services, that could bring them into contact with money laundering and terrorism financing. These include:

    (a) giving advice or administrative services in the ordering of personal affairs;

    (b) advising on the setting up of trusts, companies or other bodies;

    (c) arranging loans;

    (d) acting as a trustee, nominee or company director; and

(e) giving advice on capital structures, acquisitions and securities issues and providing safe custody services.

14. When providing such other services, the procedures undertaken in the provision of those services may facilitate judgements about, and therefore the reporting of, suspicions of money laundering or terrorism financing. The guidance in this SAP should similarly be applied to such other services.

Responsibilities of Management

15. It is management's responsibility to ensure that the entity's operations are conducted in accordance with laws and regulations. The responsibility for the prevention and detection of money laundering and terrorism financing activities rests with management through the implementation and continued operation of adequate accounting and internal control systems. Such control systems reduce but do not eliminate the possibility of money laundering and terrorism financing activities.

16. The statutory audit process does not relieve management of these responsibilities.

General Responsibilities of Auditors

17. When reporting on financial statements, auditors perform their work in accordance with the Singapore Standards on Auditing ("SSAs"). The SSAs require that auditors:

(a) carry out procedures designed to obtain sufficient appropriate audit evidence, in accordance with the SSAs, to determine with reasonable confidence whether the financial statements are free of material misstatement;

(b) evaluate the overall presentation of the financial statements, in order to ascertain whether they have been prepared in accordance with relevant legislation and accounting standards; and

(c) issue a report containing a clear expression of their opinion on the financial statements. (SSA 200 "Objective and General Principles Governing an Audit of Financial Statements").

The SSAs also require auditors to consider the need to report to an appropriate authority in particular circumstances[1].

18. The auditor is not and cannot be held responsible for the prevention of, and failure to detect, money laundering and terrorism financing activities. External auditors performing financial statement audits are less likely than other professional accountants (such as forensic accountants and accountants in management positions) to encounter signs of possible money laundering and terrorism financing.

19. The fact that an annual audit is carried out may, however, act as a deterrent. As discussed in the auditing standards, audit work includes the review of only those systems and controls on which the auditor wishes to rely for the purpose of the audit. Accordingly, an audit examination may not have identified all the internal control weaknesses that exist.

20. Furthermore, it is not the auditors' responsibility to detect suspicious activity in connection with a compliance or operational audit of an AML/ATF program or testing a Suspicious Transaction Reporting ("STR") process.

21. Misstatements in financial statements may be caused by errors, fraud or breaches of law and regulations: money laundering (which may also be connected with fraudulent activity) and terrorism financing involves a breach of law.

[1] SSA 240 "The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements" and SSA 250 "Consideration of Laws and Regulations in an Audit of Financial Statements".

22. Whilst auditors have no statutory responsibility to undertake work solely for the purpose of detecting money laundering and terrorism financing, they nevertheless need to take the possibility of money laundering and terrorism financing into account in the course of carrying out procedures relating to fraud and compliance with laws and regulations. The following sections of this SAP provides guidance concerning the effects of AML and ATF legislation on the work of auditors.

Criminal Offences

23. Details of the criminal offences under the CDSA, TSFA and Penal Code are summarised in Appendices B, C and D respectively.

24. Auditors need to ensure that they are sufficiently aware of the main provisions of the AML and ATF legislation. In particular, the auditors' attention is drawn to the following matters:

(a) *Unknowingly assisting an offence*. Services provided by accounting firms could be of value to a successful criminal transaction. These include expertise in creating corporate vehicles, trusts and other legal arrangements that facilitate money laundering or terrorist financing, and the provision of financial and fiscal advice that is often an important element in criminal schemes.

Therefore, an accounting firm could be used by criminals resulting in a risk that the accounting firm being held liable for assisting in the crime, notwithstanding that the assistance was provided unknowingly. The prosecution need not prove that a person had actual knowledge of the relevant facts (eg. knowing that the criminal's proceeds are from criminal conduct). Instead, a person can be held liable based merely on evidence showing that he had "reasonable grounds to believe" (eg. that the proceeds were derived from criminal conduct).

Statutory defences are available. However, auditors should note that the burden of establishing those statutory defences is upon the defendant, who must satisfy the Court on the balance of probabilities.

Guidance on internal procedures that firms need to establish in order to mitigate such a risk is set out in subsequent sections of this SAP. These include matters on know-your-customer ("KYC") and training.

(b) *Statutory reporting responsibilities*. It is a criminal offence for failing to report money laundering to the authorities. Reporting is mandatory even in cases where an auditor merely has reasonable grounds to suspect that money laundering has occurred. Similarly, an auditor who fails to report terrorism financing faces the prospect of criminal liability.

Guidance on the auditor's statutory reporting responsibilities, including matters on client confidentiality, indications of suspicious transactions, internal and external reporting procedures and reporting format, are set out in the subsequent sections of this SAP.

(c) *Tipping-off offence*. It is an offence to disclose any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the CDSA.

Guidance to mitigate risk of tipping-off, including communications with management, disclosures in financial statements and qualification of the auditors' report, are set out in the subsequent sections of this SAP.

25. When considering whether or not an auditor acted in a reasonable way, the Court could have regard to the requirements of SSAs and this SAP. Therefore, all auditors should be familiar with and apply the guidance in this SAP.

26. The offence of “assisting” may become relevant to auditors when suspicions of money laundering or terrorism financing exist. In normal circumstances, fulfilment of the auditor's responsibilities, including the issue of their report on an entity's financial statements, does not give rise to risk of committing the offence, even if subsequently money laundering or terrorism financing is found to have taken place. However, where the auditors discover information which could indicate to them that money laundering or terrorism financing is occurring or has occurred, they need to complete their assessment of the position (and, if appropriate, to report to the Commercial Affairs Department (“CAD”)) as discussed later in this SAP before issuing their report on the financial statements.

27. If auditors had knowledge or suspicion that an entity to which they are appointed auditors was involved in terrorism financing or the laundering of criminal proceeds, the auditors need to consider the specific circumstances, including materiality, to assess whether the auditors’ report should be modified. If auditors failed to pursue their suspicions or take other appropriate action, it might be argued that the issue of an opinion on the entity's financial statements, without the opinion being modified when the specific circumstances warrant this, enables it to present an appearance of legitimacy with the consequence that the criminal act can continue. This inference is more likely if the auditors knew that the person is or had been engaged in the crime.

28. Hence to avoid the risk of being held to have assisted a money laundering or terrorism financing activity, individual auditors report any knowledge or suspicion of money laundering through the firm's usual internal channels to an appropriate partner of the firm, who will then determine whether a report to the CAD is necessary.

Guidance on measures auditors need to establish

29. The subsequent sections provide guidance on measures that firms need to establish, and also guidance to auditors as to their responsibilities on auditing and reporting on financial statements.

30. Guidance is provided on the following matters:

    (a) Know-Your-Customer (“KYC”);

    (b) conduct of the audit;

    (c) reporting and tipping-off;

    (d) records keeping; and

    (e) training.

Know-Your-Customer (“KYC”)

31. An important element in any effective AML/ATF measure is the KYC principles. The primary objective of KYC principles is to enable effective identification and reporting of suspicious activities. The underlying assumption is that, unless you truly know your customer, and well enough to understand and anticipate that customer’s business behaviour, you can neither reasonably nor effectively distinguish unusual and possibly suspicious activity from usual and customary behavior.

32. KYC guidelines require or recommend developing a thorough understanding, through appropriate due diligence, of the true beneficial parties to transactions, the source and intended use of funds and the appropriateness and reasonableness of the business activity and pattern of transactions in the context of the business.

33. Reference should be made to SSA 315 “Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement” which requires the auditor to “obtain an understanding of the entity and its environment, including its internal control, sufficient to identify and assess the risks of material misstatement of the financial statements whether due to fraud or error, and sufficient to design and perform further audit procedures.”

34. Prior to acceptance of appointment, auditors consider the requirements and guidance of SSA 315 to obtain a preliminary knowledge of the entity and its environment, including the structure of the entity, the nature of its business, the industry, ownership and any related parties, and perceived integrity of directors and management. Following appointment, auditors perform procedures designed to identify significant changes to these matters. The requirements and guidance of SSA 315 should, in particular, be applied in conjunction with the requirements and guidance provided in SSA 240 "The Auditor’s Responsibility to Consider Fraud in an Audit of Financial Statements" and SSA 250 “Consideration of Laws and Regulations in an Audit of Financial Statements”.

35. Reference should also be made to Singapore Standard on Quality Control 1 “Quality Control for Firms That Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services Engagements” (“SSQC 1”). SSQC 1 requires the accounting firm to obtain reasonable assurance that it will only undertake or continue relationships and engagements where it has considered the integrity of the client and does not have information that would lead it to conclude that the client lacks integrity. With regard to the integrity of a client, matters that the firm considers include, for example:

    (a) The identity and business reputation of the client’s principal owners, key management, related parties and those charged with its governance.

    (b) The nature of the client’s operations, including its business practices.

    (c) Information concerning the attitude of the client’s principal owners, key management and those charged with its governance towards such matters as aggressive interpretation of accounting standards and the internal control environment.

    (d) Whether the client is aggressively concerned with maintaining the firm’s fees as low as possible.

    (e) Indications of an inappropriate limitation in the scope of work.

    (f) Indications that the client might be involved in money laundering or other criminal activities.

    (g) The reasons for the proposed appointment of the firm and non-reappointment of the previous firm.

36. The extent of knowledge a firm will have regarding the integrity of a client will generally grow within the context of an ongoing relationship with that client. Information on such matters that the firm obtains may come from, for example:

    (a) The reasons for the proposed appointment of the firm and non-reappointment of the previous firm.

    (b) Communications with existing or previous providers of professional accountancy services to the client in accordance with the ISCA and ACRA Code, and discussions with other third parties.

    (c) Inquiry of other firm personnel or third parties such as bankers, legal counsel and industry peers.

    (d) Background searches of relevant databases.

37. The knowledge obtained may alert the auditor to factors indicating a possibility of money laundering or terrorism financing, and where this is the case, the auditor assesses their reporting responsibilities in the light of information to which they have access and applies the information obtained in planning, performing and reporting on the audit.

Conduct of the audit

Planning and performing the audit

38. In planning and performing their work, auditors obtain and document an understanding of the entity and its environment, including its internal control, sufficient to identify and assess the risks of material misstatement of the financial statements whether due to fraud or error, and sufficient to design and perform further audit procedures[2] and consider whether they may place reliance upon aspects of the internal control system. Where the auditors intend to place reliance upon such internal control systems, sufficient evidence of the effective operation of the systems will be needed[3]. However, an audit performed in order to express an opinion on the view given by financial statements may not be regarded as providing assurance on the adequacy on an entity's systems or on the actual incidence of fraud or breaches of law and regulations, including money laundering and terrorism financing. As directors are responsible for the prevention and detection of money laundering or terrorism financing activities, they may therefore wish to commission more detailed investigations in particular instances of concern. However, auditors need to take the possibility of money laundering and terrorism financing into account in the course of carrying out procedures relating to fraud and compliance with laws and regulations.

39. Specific requirements and guidance on detecting material misstatements caused by fraud and breaches of laws and regulations are set out in SSA 240 “The Auditor’s Responsibility to Consider Fraud in an Audit of Financial Statements” and SSA 250 “Consideration of Laws and Regulations in an Audit of Financial Statements”.

Fraud

40. SSA 240 requires auditors to identify and assess the risks of material misstatement due to fraud at the financial statement and the assertion level; and for those assessed risks that could result in a material misstatement due to fraud, evaluate the design of the entity’s related controls, including relevant control activities, and to determine whether they have been implemented.[4] The auditors are required to maintain an attitude of professional scepticism recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor’s past experience with the entity about the honesty and integrity of management and those charged with governance. Discussion on the susceptibility of the entity’s financial statements to material misstatement due to fraud is also required to be carried out with appropriate members of the engagement team. Factors which may increase the risk of fraud occurring are noted in the Appendix to SSA 240.

41. A close connection exists between the factors giving rise to an increased risk of fraud and those indicating money laundering: an illustrative list of factors which may be indicative of both fraud and money laundering is given in Appendix E to this SAP. Consequently, where the auditors identify such circumstances, they assess the possibility of a breach of law relating to money laundering as well as that of fraud.

[2] SSA 315 ”Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement” paragraph 2.
[3] SSA 330 “The Auditor’s Procedures in Response to Assessed Risks” paragraph 23
[4] SSA 240 “The Auditor’s Responsibility to Consider Fraud in an Audit of Financial Statements” paragraph 2

Laws and regulations

42. SSA 250 requires auditors to plan and perform the audit with an attitude of professional scepticism and requires auditors to carry out specified steps to help identify possible or actual instances of non-compliance with those laws and regulations where non-compliance should be considered when reporting on financial statements. These steps consist of:

    (a) obtaining a general understanding of the legal and regulatory framework applicable to the entity and the industry and how the entity is complying with that framework;

    (b) inspecting correspondence with relevant licensing or regulatory authorities;

    (c) enquiring of the directors as to whether they are on notice of any possible instances of non-compliance with laws and regulations; and

    (d) obtaining written confirmation that management has disclosed all known actual or possible non-compliance with laws and regulations whose effects should be considered when preparing financial statements[5].

43. As explained in SSA 250, whether an act constitutes non-compliance with law or regulations is a legal determination that is ordinarily beyond the auditor's professional competence. However, auditors' training, experience and understanding of the entity and its industry may enable them to recognise that some acts coming to their attention may constitute money laundering or terrorism financing.

44. Auditors are required to be alert for all breaches of laws and regulations which come to their attention in the course of their work and to take steps to determine the appropriate response[6]. Auditors of all entities therefore need to be sufficiently aware of the main provisions of the AML and ATF legislation in order to make a careful assessment of any factors encountered in the course of their work which lead them to suspect that crime is taking place, so as to obtain sufficient information to assess the effect on the financial statements and the implications for other aspects of their audit.

Additional considerations for audits of entities in the financial sector

45. In general, AML and ATF laws and regulations are fundamental to an entity's business in the financial sector. Entities in this sector are subject to regulation by the MAS and are required to comply with the requirements of the MAS.

46. When auditing the financial statements of such entities, auditors need to review the steps taken to comply with the requirements of the MAS as part of their assessment of the arrangements to ensure compliance with laws and regulations. The auditor should also obtain a written representation from management on the steps taken, and procedures in place, to ensure compliance with the applicable requirements issued by the MAS. As set out in paragraph 10(a), the auditors should report to the MAS of any weakness in internal controls and non-compliance with legislation that come to their attention.

Reporting and Tipping-off

47. An auditor faces the prospect of criminal liability for failing to report to the authorities suspicious transactions relating to money laundering or terrorism financing.

[5] SSA 250 “Consideration of Laws and Regulations in an Audit of Financial Statements” paragraphs 13, 15, 18 and 23
[6] SSA 250 “Consideration of Laws and Regulations in an Audit of Financial Statements” paragraphs 19 and 26.

48. Suspicious transactions should be reported to the CAD and as a guide, using the indicative report content set out in Appendix F. It is therefore critically important that auditors of all entities make a careful assessment of matters which put them on notice of money laundering or terrorism financing, in order to determine what type of activity may be involved and what obligations or consequences arise.

49. When auditing the financial statements of a regulated entity (for example, a bank), auditors have a statutory duty to report to the regulator matters of material significance to its function, or other specified matters, which come to the auditor's attention in the course of their work. Any knowledge or suspicions of involvement of the entity or the entity's management in money laundering or terrorism financing, or of failure to comply with an applicable requirement of the MAS, would normally be regarded as being of material significance to a regulator and so give rise to a statutory duty to report to the regulator . In normal circumstances, auditors can assume that reporting to a regulator does not open them to a charge of tipping-off.

Confidentiality, statutory immunity and legal privilege

50. SSA 250 paragraph 38 states that the auditor's duty of confidentiality would ordinarily preclude reporting non-compliance to a third party. However, in certain circumstances, that duty of confidentiality is overridden by statute, law or by courts of law. When auditors become aware of a suspected or actual non-compliance with law and regulations which give rise to a statutory duty to report, they should make a report to the appropriate authority without undue delay.

51. Statutory immunity is granted from any legal action, criminal or civil, for breach of confidence arising from having reported suspicions of money laundering to the CAD, provided the report is made in good faith[7]. It also means that auditors, acting in good faith, are able to report suspicious transactions without the threat of subsequent legal action even if, on further investigation, it were found that there had been no offence.

52. In practice, firms establish a clearly set out internal reporting procedures. In order to avoid the risk of being held to have assisted a money laundering or terrorism financing activity, individual auditors should report any knowledge or suspicion of such criminal activity through the firm's usual internal channels to an appropriate official (eg. partner) in the firm, who will then determine whether a report to the CAD is necessary. Statutory immunity is similarly granted to these individual auditors.

53. Legal privilege can provide a defence for a professional legal adviser to a charge of failing to report suspicions of money laundering. This only applies under privileged and restricted circumstances. There may be situations where an accounting firm comes into possession of legally privileged information, such as where it has been instructed by a lawyer on behalf of its client in respect of legal proceedings. If a suspicious transaction report required under law would result in the disclosure of that information, the accounting firm should on a case-by-case basis obtain legal advice to ascertain whether the information and the accounting firm itself, under the specific circumstances, qualifies for protection for non-disclosure on grounds of legal privilege, or whether a suspicious transaction report has to be made.

Knowledge and Suspicion

54. Suspicion is not defined in the existing legislation. Case law and other sources indicate that suspicion is more than speculation but it falls short of proof or knowledge. Suspicion is personal and subjective but will generally be built on some objective foundation.

[7] The protection generally relates to reporting knowledge or suspicion of the crime, and may not extend more widely, for example to disclosure of audit working papers to an investigating officer. Firms should consider legal advice in order to avoid a breach of confidentiality where such further disclosure is requested without a court order made under the relevant law.

55. Generally speaking, knowledge or reasonable grounds to suspect is likely to include:

(a) actual knowledge;

(b) shutting one's mind to the obvious;

(c) deliberately refraining from making inquiries, the results of which one might not care to have;

(d) deliberately deterring a person from making disclosures, the content of which one might not care to have;

(e) knowledge of circumstances which would indicate the facts to an honest and reasonable person; and

(f) knowledge of circumstances which would put an honest and reasonable person on inquiry and failing to make the reasonable inquiries which such a person would have made.

56. Suspicion is a subjective concept which may be caused by a transaction or transactions or set of circumstances which to the auditors appear unusual or out of context. It can arise from a single transaction or from on-going activity over a period of time.

57. Reasonable grounds to suspect should not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. Whilst a particular sector or business may be subject to a greater degree of inherent risk of criminal activities than another sector, or the assessment of control risk in a particular entity may raise the overall risk of fraudulent, illegal or unauthorised transactions, an assessment that there is a higher than normal risk of money laundering or terrorism financing is not the same as suspecting money laundering. For example, cash-based businesses or complex overseas trust and company structures may be capable of being used to launder money, but this capability in itself is not considered to constitute "reasonable grounds". Existence of higher than normal risk factors require increased attention to gathering and evaluation of "know-your-customer" information, and heightened awareness of the risk of money laundering or terrorism financing in performing professional work, but do not of themselves require a report of suspicion to be made.

58. In order for a suspicion to be acted upon, there must be a reasonable basis in fact, so that the person concerned can show that the suspicion that money laundering or terrorism financing has occurred is honestly held and arrived at in good faith. Therefore, for reasonable grounds to suspect to come into existence, there needs to be sufficient information to advance beyond speculation that it is possible that someone is laundering money or financing terrorism, or a generalised assumption that low levels of crime (eg. not declaring all cash takings) are endemic in particular sectors.

59. The following three points may be of assistance in determining whether there are reasonable grounds for knowledge or suspicion that someone is committing a money laundering offence:

(a) Does the conduct under scrutiny fall within that which is potentially criminal?

(b) If so, is the person or entity in question suspected of having been involved in that conduct or arrangement?

(c) What factors and information have led to the formation of knowledge or suspicion, i.e. how will the grounds for the report be described to authorities?

60. In considering factors which may put auditors on notice that there is a risk that money laundering or terrorism financing may be occurring, two situations can be distinguished:

    (a) *the entity is involved knowingly and/or actively*: Auditors consider the effect of such factors, where they exist, on their assessment of audit risk for the purposes of determining the work necessary to report on the entity's financial statements. For example, factors indicating an increased risk of money laundering occurring are often similar to those indicating an increased risk of fraud; and

    (b) *the entity is inadvertently involved*: Such involvement may occur in one of two ways. The entity's directors or management may realise that an unusual transaction is taking place but have no evidence to suggest that the unusual transaction involves money laundering or terrorism financing. Alternatively, the directors or management may not even suspect that anything unusual is happening. Factors indicating an increased risk of such "third party" money laundering or terrorism financing are likely to be more difficult to distinguish from routine innocent transactions, particularly if the amounts concerned are comparatively small in the context of the entity's financial statements.

61. An illustrative list of factors which may give rise to an increased risk that either type of money laundering may be occurring are set out in Appendix E. Such factors may not come to the attention of auditors where they are not significant or material in the context of the financial statements on which they are reporting, nor is the existence of an individual factor necessarily sufficient of itself to give rise to suspicion: legitimate reasons arising in the ordinary course of business may give rise to many of the circumstances listed.

62. Money laundering or terrorism financing activity may first be identified in relation to comparatively small amounts. However, a continuous use of apparently immaterial transactions may be used to give apparent legitimacy to significant amounts of criminal proceeds. Auditors need to be alert to circumstances in which a combination of factors may give rise to suspicion and, when suspicion arises, to determine whether the matter ought to be reported to the CAD.

63. Auditors also need to bear in mind that they may not be able to identify the source of the funds, and therefore may not be able to ascertain whether the funds relate to one of the predicate crimes or terrorism financing. In case of doubt, auditors may wish to take legal advice and, subject to that advice, to report the matter to the CAD.

Procedures when possible money laundering or terrorism financing is discovered

64. SSA 250 requires auditors who become aware of a possible breach of law or regulations to obtain an understanding of the matters and the circumstances in which it has occurred, and sufficient other information so as to evaluate the possible effect on the financial statements and its implications for other aspects of the audit[8].

65. Normally, the auditors discuss the matter with appropriate members of management and the board of directors: however, SSA 250 paragraph 34 states that this step should not be taken if the auditors have concluded that they no longer have confidence in the integrity of the directors. Indications that the directors are aware of or involved in the criminal activity would be grounds for this conclusion: in addition, auditors need to be aware that they are under a statutory obligation not to disclose related information to the directors (or other parties) if doing so is likely to fall within the definition of tipping-off. Hence to avoid any risk of tipping-off it is important that the auditors only go so far as to establish to their own satisfaction whether there is a suspected case of money laundering or terrorism financing involving the directors and to consider the consequences for the report on the financial statements.

[8] SSA 250 "Consideration of Laws and Regulations in an Audit of Financial Statements" paragraphs 26, 28 and 31

66. Similarly, where the entity or its customers, suppliers or other business associates are suspected of being involved in the criminal activity, auditors undertake their assessment of the circumstances with care so as not to alert the entity's management or anyone else to these suspicions in case tipping-off occurs. Consequently, auditors need to exercise caution in determining with whom, amongst the management and directors, the suspicions can be discussed and they may conclude that none would be suitable. In cases of doubt, legal advice would normally be sought.

67. Preliminary enquiries to verify the precise nature of a transaction will not give rise to a tipping-off offence unless auditors know or suspect that an investigation is underway or is proposed and that the enquiries by the auditors are likely to prejudice that investigation. Where it is known or suspected that a report has already been made to the CAD, great care is necessary to ensure that the perpetrator does not become aware that the matter has been brought to the attention of the law enforcement agencies. When the auditors conclude that further enquiries are necessary in order to obtain sufficient audit evidence for their report on the entity's financial statements they should consider obtaining legal advice and/or consult with the CAD as to the extent and possible effect of those enquiries before undertaking further work.

68. The actions taken when considering whether to report suspicions of money laundering or terrorism financing will have a different emphasis depending on whether the entity is actively or passively involved in money laundering or terrorism financing, though this may be a difficult decision to make. In cases of doubt, it may be prudent to assume the entity is actively involved. If the entity appears to be actively involved, great care would need to be taken not to alert it to the auditor's suspicions. If the entity appears to be only passively involved, the entity's directors need to take appropriate steps to prevent further involvement; in addition, depending upon the size and complexity of the entity, its control procedures might have been expected to prevent the event occurring and so the directors need to be alerted to any weakness in the systems. However, great care still needs to be taken in case some of the entity's staff are involved or the entity alerts the third party.

69. SSQC 1, SSA 240 and SSA 250 set out requirements and guidance on withdrawal from the engagement, communication with client and responding to enquiry from the proposed in-coming auditor.

The auditor's report on financial statements

70. Misstatements in financial statements may be caused by fraud or breaches of law and regulations: money laundering (which may also be connected with fraudulent activity) and terrorism financing involves a breach of law.

71. If it is known that money laundering or terrorism financing has occurred, the auditor need to consider the specific circumstances, including materiality, to assess whether the auditor's report should be modified. The auditor should also consider the necessity of asking the CAD whether disclosure in the auditor's report on the financial statements, either through qualifying the opinion or referring to fundamental uncertainty, could constitute tipping-off. If this is the case, auditors would be in a difficult position and are likely to require legal advice as to how their responsibility to the shareholders of the entity may be discharged. Timing may be the crucial factor.

Records Keeping

72. Care is also necessary in the documentation of risk assessments relating to money laundering and any suspicions that arise during the audit. Staff need to be aware of the importance of satisfactorily clearing any points that may be raised in the course of the audit.

73. In order to assist the relevant investigating authorities, firms should maintain all relevant records pertaining to a client subject to an on-going investigation until closure of the case.

74. It is also best practice to maintain a complete file of all internal suspicious transactions reports filed by individual auditors, whether or not these were subsequently reported by the firm to the CAD and/or the MAS. Firms should ensure that there is proper justification, documented in writing, for internal suspicious transactions reports that are not subsequently reported to the CAD.

Training

75. The statutory definition of money laundering and terrorism financing can be complex. There can be wide variation in what constitutes unusual and suspicious activity and legally reportable conditions of suspicious transactions.

76. Firms should therefore establish an on-going training programme and take appropriate steps to ensure that all levels of professional staff have undergone such training. Staff should be reminded of their responsibilities and kept informed of new developments through refresher training, or through other forms of internal communication, at regular intervals.

77. A firm's training programme should be tailored to its size, nature and complexity. The extent of knowledge required by individual members of staff is determined by their role in the firm. Training would as a minimum be expected to emphasise the following:

(a) requirements of the AML and ATF legislation;

(b) policies and procedures on "know-your-customers", such as policies and procedures on client due diligence and acceptance;

(c) indications of money laundering and terrorism financing;

(d) risks of tipping-off;

(e) procedures for internal consultation and reporting of suspected money laundering and terrorism financing; and

(f) the need to obtain legal advice in situations where there is doubt about the legal framework and requirements.

78. When any individual involved in an audit has knowledge or suspicion of money laundering or terrorism financing, he or she would be expected to follow the audit firm's internal reporting procedures. Junior staff may be the first to spot evidence of crime. This reinforces the need for firms to have clear procedures which are communicated to all personnel. Staff ought to report any suspicions to an appropriate official (eg. partner) in the firm. This will discharge their personal reporting responsibility.

79. Training does not need to be performed in-house. Attendance at conferences, seminars and training courses run by external organisations, or participation in computer based training courses, may be taken to represent an effective method of fulfilling the training obligations. However, audit firms should ensure the appropriateness of those courses, seminars or conference.

APPENDIX A

DESCRIPTION OF MONEY LAUNDERING AND TERRORISM FINANCING

A1. Professionals, such as accountants, are at risk of being used by criminals for money laundering or terrorism financing purposes because their services could be of value to a successful criminal transaction or they may be used merely to give the appearance of legitimacy to a criminal transaction.

Money Laundering

A2. Money laundering is the funneling of cash or other funds generated from illegal activities through financial institutions and businesses to conceal or disguise the true ownership and source of the funds.

A3. Although money laundering can be defined and the main characteristics of money laundering can be identified, money laundering comes in widely varying forms and degrees. Usually the process of money laundering occurs in many phases and through many different transactions, thereby making identification of the process difficult if not impossible. Although the activities and methods of money laundering have become increasingly complex and ingenious, its "operations" tend to consist of three basic stages or processes — placement, layering and integration.

(a) *Placement* is the process of disposing the proceeds from drug trafficking or criminal conduct, for example by transferring the illegal funds into the financial system in a way that financial institutions and government authorities are not able to detect. Money launderers pay careful attention to national laws, regulations, governance structures, trends and law enforcement strategies and techniques to keep their proceeds concealed, their methods secret and their identities and professional resources anonymous.

(b) *Layering* is the process of generating a series or layers of transactions to distance the proceeds from their illegal source and to obscure the audit trail. Common layering techniques include outbound electronic funds transfers, usually directly or subsequently into a "bank secrecy haven" or a jurisdiction with lax record-keeping and reporting requirements, and withdrawals of already-placed deposits in the form of highly liquid monetary instruments, such as money orders or travelers checks.

(c) *Integration*, the final money-laundering stage, is the unnoticed reinsertion of successfully laundered, untraceable funds into an economy. This is accomplished by spending, investing and lending, along with cross-border, legitimate-appearing transactions.

Terrorism Financing

A4. Terrorism financing refers to the direct or indirect act of providing or collecting property for terrorist acts, providing property and services for terrorist purposes, using or possessing property for terrorist purposes, and dealing with property of terrorists. Properties refer to assets of every kind, whether tangible or intangible, movable or immovable, including bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit.

A5. Given its nature, signs of suspicious activities relating to terrorism financing is generally less observable. The assets involved in the transaction may not necessarily be proceeds from criminal activities. These assets could also be derived from lawful activities but intended for use in support of terrorism.

A6. A terrorist refers to any person who commits or attempts to commit any terrorist act, or participates in or facilitates the commission of any terrorist act. A terrorist act includes, among others, actions that involve violence against a person, serious damage to property, endangering a person's life, creating a serious risk to the health or the safety of the public, the use of firearms or explosives, and releasing into the environment dangerous, hazardous, radioactive or harmful substance.

APPENDIX B

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER ANTI-MONEY LAUNDERING LEGISLATION

B1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel should be sought where appropriate or necessary.

B2. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act ("CDSA") contains seven basic offences directly in relation to money laundering:

(a) laundering own benefits from drug trafficking or criminal conduct;

(b) assisting another to launder benefits from drug trafficking or criminal conduct;

(c) laundering by acquisition;

(d) assisting another to retain or control the benefits of drug trafficking or criminal conduct;

(e) failure to report suspicious transactions;

(f) tipping-off offence; and

(g) failure to co-operate with law enforcement agencies.

B3. Drug trafficking includes offences relating to the manufacturing, importation and exportation of controlled drug, and cultivation of cannabis, opium and coca plants. Criminal conduct refers to serious crimes as defined under the CDSA. There are many offences that have been defined as serious offences under the CDSA and these include bribery, corruption, criminal breach of trust, theft, misappropriation of property and cheating.

B4. The auditors' attention is specifically drawn to the extra-territorial provisions of the CDSA. The terms "drug trafficking" and "criminal conduct" include offences that are committed outside Singapore, as defined under the CDSA.

B5. The following sets out a summary of the seven basic offences.

Laundering own benefits from drug trafficking or criminal conduct

B6. It is an offence for a person[9] to conceal or disguise property which is, in whole or in part, directly or indirectly, represents, his own benefits from drug trafficking or criminal conduct. The offence extends to steps to convert or transfer that property, or to remove it from the Singapore jurisdiction.

B7. There are no statutory defences. Upon conviction, the accused faces a fine not exceeding $200,000, or imprisonment for a term not exceeding 7 years, or both.

[9] The legislation's use of the term 'person' indicates that commission of an offence by a legal body, as well as by an individual, is not excluded.

Assisting another to launder benefits from drug trafficking or criminal conduct

B8. Any person who, knowing or having reasonable grounds to believe that any property is, in whole or in part, directly or indirectly, represents, another person's benefits from drug trafficking or criminal conduct:

(a) conceals or disguises that property; or

(b) converts or transfers that property or removes it from the Singapore jurisdiction,

for the purpose of assisting any person to avoid prosecution for drug trafficking, criminal conduct or the making or enforcement of a confiscation order shall be guilty of an offence.

B9. Upon conviction, the accused faces a fine not exceeding S$200,000 and/or imprisonment for a term not exceeding 7 years.

Laundering by acquisition

B10. It is an offence to acquire any property for no or inadequate consideration, knowing or having reasonable grounds to believe that the property represents another person's benefits of drug trafficking or criminal conduct.

B11. Upon conviction, the accused faces a fine not exceeding S$200,000 and/or imprisonment for a term not exceeding 7 years.

Assisting another to retain or control the benefits of drug trafficking or criminal conduct

B12. It is an offence for an auditor to enter into or otherwise be concerned in an arrangement knowing or having reasonable grounds to believe that by that arrangement:

(a) it will facilitate the retention or control of benefits of drug trafficking or criminal conduct by/on behalf of; or

(b) the benefits of drug trafficking or criminal conduct are used to secure funds or acquire property (by way of investment or otherwise) for,

another person (whom the auditor knows or has reasonable grounds to believe has been/is involved in, or has benefited from, drug trafficking or criminal conduct).

B13. The following are statutory defences to charges of committing the above offence:

(a) the person proves that he did not know and had no reasonable ground to believe that the arrangement related to any person's proceeds from drug trafficking or criminal conduct, or facilitated the criminal to use, retain or control the property;

(b) before acting in connection with any arrangement, the person discloses the knowledge or suspicion of money laundering to either (i) an authorised officer; or (ii) to an appropriate person/partner following the accounting firm's internal procedure and, thereafter, if that person only acts with the consent of the authorised officer;

(c) where the person has begun to act/has acted in connection with any arrangement, the person discloses the knowledge or suspicion on his own initiative and as soon as it is reasonable to either (i) an authorised officer; or (ii) to an appropriate person/partner following the accounting firm's internal procedure; or

(d) the person proves that he intended to disclose his suspicion or belief of money laundering to an authorised officer[10] and that there is a reasonable excuse for his failure to do so.

The term "reasonable excuse" permits a Court to take account of any factor which would be considered reasonable in all the circumstances of a particular case. Justifiable fear of physical violence or other menaces may be regarded as reasonable in this context: however, the meaning of the term "reasonable excuse" is wider than physical distress and may include other factors, depending upon the circumstances - for example, practical difficulties of making a report or deciding to obtain further information before doing so.

Failure to report suspicious transactions

B14. It is mandatory for all persons who, in the course of their trade, profession, business or employment, know or have reasonable grounds to suspect that any property representing the proceeds of drug trafficking or criminal conduct or was used (or is intended to be used) in connection with drug trafficking or criminal conduct, to disclose such knowledge or suspicion to an authorised officer as soon as is reasonably practicable after it comes to his attention.

B15. Failure to report the knowledge or suspicion is an offence punishable by a fine of up to $10,000.

Tipping-off offence

B15. It is an offence to disclose any information to any person if doing so is likely to prejudice an investigation or proposed investigation under the CDSA. Disclosure in such circumstances is also known as 'tipping-off'.

B16. The offence is committed if a person knows or has reasonable grounds to suspect:

(a) that an authorised officer is acting/proposing to act in connection with an investigation which is being or is about to be conducted; or

(b) that a disclosure has been made to an authorised officer,

and he discloses any information to any person which is likely to prejudice any investigation, proposed investigation or potential investigation, as the case may be.

B17. Tipping-off offence is punishable by a fine of up to $30,000, or imprisonment of up to three years, or both.

B18. It is a defence for a person accused of tipping-off to prove that he did not know or suspect that the disclosure was likely to be prejudicial to such an investigation or that he had lawful authority for making the disclosure.

Failure to co-operate with the law enforcement agencies

B19. An authorised officer can apply to the Court for a production order requiring a person to produce relevant materials or allow authorised officers to have access to such materials. The CDSA also empowers the Court to issue a warrant authorising an authorised officer to enter and search a specified premises.

B20. It is an offence to contravene a production order issued by the Court, or obstruct or hinder any authorised officer acting in the discharge of his duty under the CDSA.

[10] Under the CDSA, an "authorised officer" is defined to mean any officer of the Central Narcotics Bureau appointed under the Misuse of Drugs Act; any special investigator of the Corrupt Practices Investigation Bureau appointed under the Prevention of Corruption Act; any Commercial Affairs Officer appointed under the Police Force Act 2004; any police officer; or any officer authorised by the Minister under the CDSA. Officers of the Commercial Affairs Department ("CAD") are authorised officers under the Act. Reports should normally be made to the Suspicious Transaction Reporting Office ("STRO") of the CAD, which provides a national reception point for all reports concerning known or suspected money laundering and terrorism financing.

APPENDIX C

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER TERRORISM-FINANCING LEGISLATION

C1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel should be sought where appropriate or necessary.

C2. The Terrorism (Suppression of Financing) Act ("TSFA") contains six basic offences:

(a) providing or collecting property for terrorist acts;

(b) providing property and services for terrorist purposes;

(c) using or possessing property for terrorist purposes;

(d) dealing with property of terrorists;

(e) failure to report terrorism financing offences; and

(f) failure to co-operate with the law enforcement agencies.

Terrorism financing offences include conspiracy, inciting another and attempting to commit, and aiding, abetting, counselling or procuring the commission of, offences C2(a) to C2(d).

C3. The term "property" means assets of every kind, whether tangible or intangible, movable or immovable. This means that money, property, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, would all constitute property under the TSFA. A property is deemed to be terrorist property if the property is used, in whole or in part, in order to commit any terrorist act.

C4. A "terrorist" refers to any person who commits/attempts to commit any terrorist act, or participates in or facilitates the commission of any terrorist act. A terrorist includes any person defined in regulations made under the United Nations Act (Cap. 339). Currently, the Schedule of the United Nations (Anti-Terrorism Measures) Regulations 2001 ("UN Regulations") contains a list of persons identified to be a terrorist. One can check the list of terrorist names under the Schedule of the UN Regulations to determine if he is in possession, custody or control of property belonging to any person identified to be terrorists. A list of terrorists can also be found in the Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations 2002.

C5. A "terrorist act" includes, among others, actions that involve violence against a person, serious damage to property, endangering a person's life, creating a serious risk to the health or the safety of the public, the use of firearms or explosives, and releasing into the environment dangerous, hazardous, radioactive or harmful substance.

C6. The auditors' attention is specifically drawn to the extra-territorial provision of the TSFA. It provides for extra-territorial jurisdiction for offences C2(a) to C2(c) committed outside Singapore by any person. Where a Singapore citizen commits an offence outside Singapore relating to the dealing with terrorist property or failure to report terrorism financing (that is, offences C2(d) and C2(e)), he may be dealt with as if the offence had been committed in Singapore.

C7. The following sets out a summary of the six basic offences.

Providing or collecting property for terrorist acts

C8. It is an offence for any person to directly or indirectly, wilfully and without lawful excuse, provides or collects property:

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

(b) knowing or having reasonable grounds to believe that the property will be used,

to commit any terrorist act.

C9. Upon conviction, the accused faces a fine of up to $100,000, or imprisonment of up to 10 years, or both.

Providing property and services for terrorist purposes

C10. It is an offence for any person to, directly or indirectly, collect property, provide or invite a person to provide, or make available property or financial or other related services:

(a) intending that they be used, or knowing or having reasonable grounds to believe that they will be used for the purpose of facilitating or carrying out any terrorist act, or for benefiting any person who is facilitating or carrying out such an activity; or

(b) knowing or having reasonable grounds to believe that they will be used by or will benefit any terrorist or terrorist entity.

C11. Upon conviction, the accused faces a fine of up to $100,000, or imprisonment of up to 10 years, or both.

Using or possessing property for terrorist purposes

C12. It is an offence for any person to:

(a) use property, directly or indirectly, for the purpose of facilitating or carrying out any terrorist act; or

(b) possess property intending that it be used or knowing or having reasonable grounds to believe that it will be used, directly or indirectly, for the purpose of facilitating or carrying out a terrorist act,

C13. Upon conviction, the accused faces a fine of up to $100,000, or imprisonment of up to 10 years, or both.

Dealing with property of terrorists

C14. Except where specific exemption (subject to terms and conditions) is granted by a lawful authority under the TSFA, no person in Singapore and no citizen of Singapore outside Singapore shall:

(a) deal, directly or indirectly, in any property that he knows or has reasonable grounds to believe is owned/controlled by or on behalf of any terrorist or terrorist entity, including funds derived or generated from property owned/controlled, directly or indirectly, by any terrorist or terrorist entity;

(b) enter into or facilitate, directly or indirectly, any financial transaction related to a dealing in property referred to in paragraph (a); or

(c) provide any financial services or any other related services in respect of any property referred to in paragraph (a) to, or for the benefit of, or on the direction or order of, any terrorist or terrorist entity.

C15. Upon conviction, the accused faces a fine of up to $100,000, or imprisonment of up to 10 years, or both.

Failure to report terrorism financing offences

C16. The TSFA imposes a duty on every person in Singapore and every Singapore citizen outside Singapore who has possession, custody or control of terrorist property, or information regarding a transaction/proposed transaction in terrorist property to disclose such information to the authorities.

C17. The TSFA also requires every person in Singapore who has information which he knows or believes may be of material assistance in preventing a terrorism financing offence, or in securing the apprehension, prosecution or conviction of a person for a terrorism financing offence, to immediately inform the authorities.

C18. Failure to report is an offence punishable by a fine of up to $50,000, or imprisonment of up to 5 years, or both.

Failure to co-operate with the law enforcement agencies

C19. The TSFA has provisions allowing the Court to issue search warrants, seizure warrants, forfeiture orders or restraint orders against terrorist property. The TSFA also empowers the relevant authorities to require a person to furnish such information or particulars as the relevant authorities think fit in relation to a report of terrorism financing offence.

C20. Failure to co-operate in relation to those matters is an offence.

APPENDIX D

SUMMARY OF BASIC CRIMINAL OFFENCES UNDER THE PENAL CODE

D1. This summary is not a reproduction of the actual wordings in the legislation. It is only intended to provide a broad description of the key legal provisions and, therefore, does not constitute authoritative legal interpretation of the legislation. Legal counsel should be sought where appropriate or necessary.

D2. The primary legislation in Singapore contains the offence of abetment indirectly in relation to an offence. The nature of this offence is summarised below.

D2. The offence of abetment is set out in sections 107, 108 and 108A of the Penal Code. Abetment involves the active involvement of a person with the principal culprit towards the commission of an offence. There are three forms of abetment, namely:

(a) abetment by instigation;

(b) abetment by conspiracy; and

(c) abetment by aid.

D3. A person who knowingly aids an offence or facilitates an offence would be liable for abetment of that offence. In the case of *Mavuthalayan (1934) 58 Mad 86* it was held that a person who knowingly aids in the disposal of stolen property is an accomplice to the offence. Therefore, for example, a person who knowingly disposes of, or conceals, (that is, launders) the proceeds of an illegal gambling house may be liable for abetting an offence under the Common Gaming Houses Act (Cap. 49).

D4. Depending on the facts and circumstances, a person who launders money may be convicted for abetment by aid.

APPENDIX E

FACTORS INDICATING AN INCREASED RISK OF MONEY LAUNDERING

E1. Money launderers use many different and sophisticated types of schemes, techniques and transactions to accomplish their ends. While it would be difficult to describe all money laundering methodologies, the following are the more frequently observed signs of suspicions:

(a) broadly, transactions that appear inconsistent with a client's known legitimate (business or personal) activities or means; unusual deviations from normal account and transaction;

(b) any situation where personal identity is difficult to determine;

(c) unauthorised or improperly recorded transactions; inadequate audit trails;

(d) unconventionally large currency transactions, particularly in exchange for negotiable instruments or for the direct purchase of funds transfer services;

(e) apparent structuring of transactions to avoid dealing with identification requirements or regulatory record-keeping and reporting thresholds;

(f) transactions passed through intermediaries for no apparent business reason; and

(g) introduction of a client by an overseas associate or financial institution based in a country or jurisdiction known for drug trafficking and production, other financial crimes and “bank secrecy”.

E2. The following sets out examples of factors indicating increased risk of money laundering. These include industry-specific indicators that auditors may come across during their audit work.

E3. **Common Indicators**

(a) **General**

- Frequent address changes.
- Client does not want correspondence sent to home address.
- Client repeatedly uses an address but frequently changes the names involved.
- Client uses a post office box or general delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after he/she has opened an account.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls, policies and reporting; client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client has only vague knowledge of the amount of a deposit.
- Client gives unrealistic, confusing or inconsistent explanation for transaction or account activity.
- Defensive stance to questioning or over-justification of the transaction.
- Client is secretive and reluctant to meet in person.
- Unusual nervousness of the person conducting the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client insists on a transaction being done quickly.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.

- Client offers money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- Client attempts to convince employee not to complete any documentation required for the transaction.
- Large contracts or transactions with apparently unrelated third parties, particularly from abroad.
- Large lump-sum payments to or from abroad, particularly with countries known or suspected to facilitate money laundering activities.
- Client is quick to volunteer that funds are “clean” or “not being laundered.”
- Client’s lack of business knowledge atypical of trade practitioners.
- Forming companies or trusts with no apparent business purpose.
- Unusual transference of negotiable instruments.
- Uncharacteristically premature redemption of investment vehicles, particularly with requests to remit proceeds to apparently unrelated third parties or with little regard to tax or other cancellation charges.
- Large or unusual currency settlements for investments or payment for investments made from an account that is not the client’s.
- Clients seeking investment management services where the source of funds is difficult to pinpoint or appears inconsistent with the client’s means or expected behavior.
- Purchase of large cash value investments, soon followed by heavy borrowing against them.
- Buying or selling investments for no apparent reason, or in circumstances that appear unusual, e.g., losing money without the principals seeming concerned.
- Forming overseas subsidiaries or branches that do not seem necessary to the business and manipulating transfer prices with them.
- Extensive and unnecessary foreign travel.
- Purchasing at prices significantly below or above market.
- Excessive or unusual sales commissions or agents fees; large payments for unspecified services or loans to consultants, related parties, employees or government employees.

(b) **Cash Transactions**

- Client frequently exchanges small bills for large ones.
- Deposit of bank notes with a suspect appearance (very old notes, notes covered in powder, etc).
- Use of unusually large amounts in traveler’s checks.
- Frequent domestic and international ATM activity.
- Client asks to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Purchase or sale of gold, diamonds or other precious metals or stones in cash.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).

(c) **Transactions Involving Accounts**

- Apparent use of personal account for business purposes.
- Opening accounts when the client’s address is outside the local service area.
- Opening accounts with names very similar to other established business entities.
- Opening an account that is credited exclusively with cash deposits in foreign currencies.
- Use of nominees who act as holders of, or who hold power of attorney over, bank accounts.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.

- Funds being deposited into several accounts, consolidated into one and transferred outside the country.
- Use of wire transfers and the Internet to move funds to/from high-risk countries and geographic locations.
- Accounts receiving frequent deposits of bearer instruments (e.g., bearer cheques, money orders, bearer bonds) followed by wire transactions.
- Deposit at a variety of locations and times for no logical reason.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Cash advances from credit card accounts to purchase cashier's checks or to wire funds to foreign destinations.
- Large cash payments on small or zero-balance credit card accounts followed by "credit balance refund checks" sent to account holders.
- Attempting to open accounts for the sole purpose of obtaining online banking capabilities.

(d) **Transactions Related to Offshore Business Activity**

- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.

E4. Industry-Specific Indicators

(a) **Financial Entities**

Personal Transactions

- Client makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account).
- Client runs large credit card balances.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.
- Client has numerous accounts and deposits cash into each of them, with the total credits being a large amount.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client acquires significant assets and encumbers them with security interests that do not make economic sense.

Corporate and Business Transactions

- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them to have such contact.
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Client makes a single and substantial cash deposit composed of many large bills.

- Asset acquisition is accompanied by unusual security arrangements.

(b) **Businesses that Provide Loans**

- Client suddenly repays a problem loan unexpectedly.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.

(c) **Life Insurance Companies, Brokers and Agents**

- Atypical incidence of pre-payment of insurance premiums.
- Insurance policies with premiums that exceed the client's apparent means.
- Insurance policies with values that appear to be inconsistent with the client's insurance needs,
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Client conducts a transaction that results in a conspicuous increase in investment contributions.
- Client shows more interest in the cancellation or surrender than in the long-term results of investments.
- The duration of the life insurance contract is less than three years.
- The first (or single) premium is paid from a bank account outside the country.
- Client accepts very unfavorable conditions unrelated to his or her health or age.
- Transaction involves use and payment of a performance bond resulting in a cross border payment.
- Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder.

(d) **Securities Dealers**

- Attempts to purchase investments with cash.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Large fund flows through non-resident accounts with brokerage firms.
- Transaction of very large dollar size.
- Unusually complex method of purchasing financial products.
- All principals of client are located outside of local jurisdiction.
- Third-party purchases of shares in other names (i.e., nominee accounts).

(e) **Foreign Exchange Dealers and Money Services Businesses**

- Client exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Client knows little about address and contact details for payee, is reluctant to disclose this information or requests a bearer instrument.
- Client wants a cheque issued in the same currency to replace the one being cashed.
- Client instructs that funds are to be picked up by a third party on behalf of the payee.
- Client requests numerous cheques or postal money orders in small amounts and various names, which total the amount of the exchange.

(f) **Accountants**

- Use of many different firms of auditors and advisers for connected companies and businesses.
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

(g) **Real Estate Brokers or Sales Representatives**

- Client arrives at a real estate closing with a significant amount of cash.
- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Client purchases property without inspecting it.
- Client purchases multiple properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Client is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided.

(h) **Casinos and other Gaming/Betting Organizations**

- Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party.
- Client requests checks that are not for gaming winnings.
- Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino check.
- Client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or checks.

(i) **Factors arising from action by the entity or its directors**

Where an entity is actively involved in money laundering, the signs are likely to be similar to those where there is a risk of fraud, and include:

- complex corporate structure where complexity does not seem to be warranted;
- complex or unusual transactions, possibly with related parties;
- transactions with little commercial logic taking place in the normal course of business;
- transactions not in the normal course of business;
- transactions where there is a lack of information or explanations, or where explanations are unsatisfactory;
- transactions at an undervalue;

- transactions with companies whose identity is difficult to establish as they are registered in countries known for their commercial secrecy;
- extensive or unusual related party transactions;
- many large cash transactions when not expected;
- payments for unspecified services, or payments for services that appear excessive in relation to the services provided;
- the forming of companies or trusts with no apparent commercial or other purpose;
- long delays in the production of company or trust accounts;
- foreign travel which is apparently unnecessary and extensive.

(j) Politically Exposed Persons ("PEPs")

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example:

- Heads of State or of government
- senior politicians
- senior government judicial or military officials
- senior executives of state owned corporations
- important political party officials.

Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

APPENDIX F

INDICATIVE REPORT CONTENT

Reporting Accounting Firm	
Name:	
Address:	
Telephone:	
Reporting Officer	
Name of Reporting Officer:	
Designation:	
Report Reference:	
Contact Officer: (if different from Reporting Officer)	
Designation:	
Customer's Particulars	
Name:	
Country of Registration:	
Registration Date:	
Registration No.:	
Address:	
Telephone:	
Name of CEO:	

* Delete whichever is inappropriate.

Suspicious Transaction(s)		
Amount	**Date**	**Description of Transaction (E.g. Funds transfer, source of funds, destination, etc.)**

Reason(s) for Suspicion:

Other Relevant Information (Including Any Actions Taken):

A copy of the following documents are attached:
☐ Customer Identification Documents
☐ Relevant Documents Supporting the Suspicious Transactions

_____

(Signature of Reporting Officer)

Date: