Financial Action Task Force

Groupe d'action financière

THIRD MUTUAL EVALUATION REPORT
ANTI-MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM

SINGAPORE

29 FEBRUARY 2008

TABLE OF CONTENTS

PREFACE - INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF SINGAPORE

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of Singapore was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[1]. The evaluation was based on the laws, regulations and other materials supplied by Singapore, and information obtained by the assessment team during its on-site visit to Singapore from 3-14 September 2007, and subsequently. During the on-site, the assessment team met with officials and representatives of all relevant Singapore government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the mutual evaluation report.

2. The evaluation was undertaken by a joint FATF/APG assessment team consisting of representatives from the FATF and APG Secretariats, FATF experts in criminal law, law enforcement and regulatory issues and an APG financial expert. The team was led by Valerie Schilling, Principal Administrator of the FATF Secretariat and Gordon Hook, Executive Secretary of the APG Secretariat, and included: Kevin Vandergrift, Administrator of the FATF Secretariat; John Ellis, Technical Specialist, Financial Crime Operations Team, Financial Services Authority, United Kingdom (financial expert); Judith Schmidt, Deputy Head, Anti-Money Laundering Control Authority Federal Finance Administration (FFA), Switzerland (financial expert); Kazuhiro Sakamaki, Deputy Director, International Affairs Office, Financial Services Agency, Japan (financial expert); Jean B. Weld, Senior Trial Attorney, Asset Forfeiture and Money Laundering Section, U.S. Department of Justice (legal expert); and Wayne Eacott, Financial Investigations Team, Perth Office, Economic & Special Operations, Australian Federal Police (AFP), Australia (law enforcement expert). The assessment team reviewed the institutional framework, relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.

3. This report summarises the AML/CFT measures in place in Singapore as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out Singapore's levels of compliance with the FATF 40+9 Recommendations (Table 1), and provides recommendations on how certain aspects of the system could be strengthened (Table 2).

[1] As updated in February 2007.

EXECUTIVE SUMMARY

1. Background Information

1. This report summarises the anti-money laundering (AML)/combating the financing of terrorism (CFT) measures in place in Singapore as of the time of the on-site visit (3-14 September 2007), and shortly thereafter. The report describes and analyzes those measures and provides recommendations on how certain aspects of the system could be strengthened. It also sets out Singapore's levels of compliance with the Financial Action Task Force (FATF) 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).

2. Singapore is a major financial centre in the Asia/Pacific region. In general, the domestic crime rate is low in Singapore which is largely attributable to the deterrent effect of stringent and effective law enforcement. However, as a developed, open and stable economy located in South East Asia, Singapore faces a range of regional and international money laundering and terrorist financing risks, including capital flight associated with corruption in other South East Asian countries, as well as the proceeds of crime from a range of other offences. The size and growth of Singapore's private banking and assets management sector poses a significant money laundering (ML) risk based on known typologies. There are also terrorist financing risks. The authorities have taken action against Jemaah Islamiyah and its members and have identified and frozen terrorist assets held in Singapore. Following a security operation that commenced in December 2001, Singapore dismantled the local Jemaah Islamiyah terrorist network and confirmed that the network is no longer carrying out its activities in Singapore and that the amount of terrorist funds held in Singapore was small. Singapore continues to actively monitor for potential terrorism-related activities that may occur in Singapore.

3. Singapore's AML/CFT efforts are centered on having a sound and comprehensive legal, institutional, policy and supervisory framework, maintaining a low domestic crime rate, fostering an intolerance for domestic corruption, ensuring an efficient judiciary, and preserving a long established culture of compliance and effective monitoring of the measures implemented. Singapore has systematically taken steps to address many of the recommendations that were made in its second FATF mutual evaluation in 1998-1999. In particular, the creation of a financial intelligence unit (FIU) and the implementation of a comprehensive suspicious transaction reporting regime have significantly improved Singapore's ability to combat ML/FT. Legally binding AML/CFT Notices that clearly set out comprehensive AML/CFT requirements and provide practical guidance on how these obligations are to be fulfilled have also been issued to different classes of financial institutions. Institutional efforts to improve feedback to financial institutions, enhance supervisory oversight and step up training have also resulted in a significant overall strengthening of Singapore's AML/CFT regime. Singapore's ability to provide mutual legal assistance has also been greatly improved. However, there are remaining concerns about the effectiveness of the money laundering offence and the new cross-border declaration system, the requirements applicable to designated non-financial businesses and professions (DNFBPs), and the availability of beneficial ownership information in relation to legal persons and arrangements.

2. Legal Systems and Related Institutional Measures

4. Singapore has criminalized ML in eight separate provisions of the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA). Singapore's money laundering offences cover the conversion or transfer, concealment or disguise, possession and acquisition of property in a manner that is largely consistent with the 1988 United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organized Crime (Palermo Convention). There is

one minor technical deficiency in relation to the third-party laundering offences. Singapore has adopted a list approach to define the scope of predicate offences. At the time of the evaluation, there were 335 predicate offences for money laundering. There is a broad range of ancillary offences to the money laundering offences. Money laundering applies to both natural and legal persons, and proof of knowledge can be derived from objective factual circumstances. Natural persons are liable to a maximum fine of 500 000 Singapore Dollars (SGD) and/or imprisonment of up to seven years, while legal persons are liable to a maximum fine of SGD 1 000 000. Overall, the money laundering offence is not effectively implemented, given the overall low number of prosecutions and convictions and the size of Singapore's financial sector. The statistics suggest that Singapore is more focused on prosecuting predicate offences (primarily based on domestic crime). Singapore has, generally, been less aggressive in pursuing money laundering as a separate crime in the past, particularly in relation to third-party laundering, through Singapore's financial system, of proceeds generated by foreign predicate offences.

5. Singapore has criminalised four main terrorist financing offences in its Terrorism (Suppression of Financing) Act (TSOFA). These provisions cover the collection or provision of funds with the intention that they be used by a terrorist or terrorist organisation, or to carry out a terrorist act. The definition of "property" in the TSOFA is identical to the definition of "funds" in Article 1 of the UN International Convention for the Suppression of the Financing of Terrorism (FT Convention). Natural persons are liable to a maximum fine of SGD 100 000 and/or imprisonment of up to ten years, while legal persons are liable to a maximum fine of SGD 100 000. While there have been FT investigations, there have not been any prosecutions or convictions, and so the effectiveness of these provisions cannot be assessed.

6. Confiscation provisions are comprehensive as ancillary to criminal prosecutions. Restraint provisions are generally comprehensive as well; however, they do not adequately cover intended instrumentalities or property of corresponding value of instrumentalities. Moreover, given the risk of money being laundered in Singapore (particularly the proceeds of foreign predicate offences), the amount of money being frozen and seized seems low. Confiscation of terrorist-related property may occur without the necessity of ancillary criminal proceedings.

7. The basic provisions to prevent financial institutions and other persons from dealing with terrorist-related assets are contained in the UN (Anti-Terrorism Measures) Regulations (UN (ATM) Regulations), the Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations (2002) (MAS (ATM) Regulations), and TSOFA. They prohibit dealing, directly or indirectly, in any property that a person knows or has reasonable grounds to believe is owned or controlled by or on behalf of any terrorist or terrorist entity. They also prohibit entering into or facilitating any financial transaction related to a dealing in such property, or providing any financial services or any other related services in respect of any terrorist or terrorist organization. The term "terrorist" is defined broadly, and the schedules to the regulations reference the 1267 list. There are adequate processes in place, and although they have not yet done so, Singapore authorities can easily amend the schedule should they choose to designate terrorists of their own. Singapore has, pursuant to foreign requests, successfully used the general provisions in the regulations and in the Criminal Procedure Code (CPC) to seize funds of persons not on the 1267 list.

8. The Suspicious Transaction Reporting Office (STRO) is Singapore's financial intelligence unit. STRO was formally established on 10 January 2000 as an enforcement-style FIU under the Financial Investigation Division (FID) of the CAD in the Singapore Police Force (SPF). In 2006, STRO developed and implemented a STR On-Line Lodging System (STROLLS) for filers of suspicious transaction reports (STR). STRO also provides extensive general guidance on STR reporting on its website and through its various publications including the latest ML/TF trends, feedback on typologies, indicators of suspicious transactions and statistics. STRO has direct on-line and instantaneous access to all enforcement information including criminal records maintained by SPF. STRO officers have access to a wide variety of public record information and by the use of their coercive police powers (*e.g.* their power under section 58 of the Criminal Procedure Code (CPC) to

directly obtain the production of relevant evidence), and can obtain information from financial institutions, including financial records. STRO officers, as police officers, may exercise police powers in various situations during the course of investigating an STR. These powers are exercised in order to develop the STR and to identify the possible commission of a money laundering offence or other offences. STRO is successful at identifying domestic predicate offences through its analysis. However, given the potential attractiveness of Singapore as a large, stable and sophisticated financial centre through which to launder money, STRO is encouraged to more strongly focus on the identification of money laundering from foreign predicate offences.

9. The Financial Investigation Branch (FIB), located within the Financial Investigation Division of CAD, is the lead enforcement agency in ML/FT investigations within the SPF. The key role of FIB is to handle money laundering investigations and provide cross-jurisdiction assistance relating to ML for matters under the purview of the SPF. The work of the FIB is complemented by its sister unit in the SPF, the Proceeds of Crime Unit (PCU). The Central Narcotics Bureau (CNB) is also authorised to investigate ML offences, and has established its own specialist investigative unit (the FIT) to investigate ML offences that are related to drug trafficking. Officers of the FIB, PCU and the SPF are empowered under the CPC, CDSA and TSOFA to exercise comprehensive investigative powers, including powers of search, and seizure of evidence in relation to ML, TF or predicate offences. Overall, the regime for investigating ML has not been effectively implemented, as is illustrated by the low number of ML investigations. Although, in the past, it appears that insufficient attention has been paid to pursuing ML offences, the situation seems to be improving. The statistics do show a general increase in the number of ML investigations, with 46 "full scale" ML investigations in 2007 (as at 14 November).

10. With regard to detecting and deterring cross-border movements related to ML or FT, as of 1 November 2007, Singapore has implemented a declaration system which complements (rather than replaces) a disclosure system that Singapore has had in place since November 2004. Although the technical components of the new declaration system are comprehensive, they are too recent to be assessed for their effectiveness.

3. Preventive Measures – Financial Institutions

11. The Singapore regulatory structure utilises laws ("Acts"), regulations, and notices, all of which are enforceable. The AML/CFT Notices, issued by the Monetary Authority of Singapore (MAS) and which establish most of the AML/CFT requirements for most financial institutions as described below, are not "law or regulation" according to the FATF definition. However, they are clearly "other enforceable means", as they create legally enforceable obligations, to which criminal sanctions apply for non-compliance. There are separate Notices applicable to each financial sector; however, the language therein is virtually identical.

12. The Notices also use almost identical language to that used in the FATF Recommendations and AML/CFT Methodology. This means that, overall, preventative measures for the financial sector generally meet a high level of compliance with the detailed provisions of the FATF 40 + 9 Recommendations. Only commodities futures brokers are not yet covered for AML/CFT purposes. [2] In addition, new rules for moneylenders entered into force on 12 November 2007, so their effectiveness cannot yet be assessed. Both of these sectors comprise very small firms that are few in number, and the Monetary Authority of Singapore (MAS) (which regulates the financial sector) views both as being relatively low risk for AML/CFT purposes.

13. Existing customer due diligence (CDD) measures are generally comprehensive and are effectively applied by financial institutions. This includes customer identification and verification,

[2] With effect from 27 February 2008, MAS assumed regulatory oversight of commodity futures: http://www.mas.gov.sg/legislation_guidelines/securities_futures/sub_legislation/Publication_of_MAS_Regulations_and_Notices_on_the_Transfer_of_Regulatory_Oversight_of_Commodity_Futures.html.

beneficial ownership requirements, and measures for politically exposed persons (PEPs), correspondent banking, and new technologies and non-face to face customers. The main issue is that basic CDD requirements are not laid out in "law or regulation" as required by the FATF standards but rather in the Notices which are "other enforceable means." Requirements for introduced business are generally comprehensive as well; however, financial institutions are not specifically required to immediately obtain CDD information on introduced customers.

14. Record keeping requirements are comprehensive and are generally observed; however, the requirements for financial institutions to maintain business correspondence, and the requirement for money exchange and remittance businesses to maintain identification data should be laid out in law or regulation. Wire transfer provisions are also broad, and secrecy provisions do not inhibit implementation of the FATF standards.

15. Financial institutions are required to pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose, inquire into the background and purpose of such, and document their findings with a view to making this information available to the relevant competent authorities should the need arise. Financial institutions are further required to give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the financial institutions for themselves or notified to financial institutions generally by MAS or other foreign regulatory authorities. However, in relation to those countries which continue not to apply or insufficiently apply the FATF recommendations, no enforceable powers have been exercised to require financial institutions to apply stringent or additional AML/CFT counter-measures.

16. The CDSA requires that any person who, in the course of his/her professional or business duties, knows or has reasonable grounds to suspect that any property represents the proceeds of drug trafficking or criminal conduct (as defined in section 2(1) of the CDSA), or was used or is intended to be used in connection with drug trafficking or criminal conduct (which includes ML/FT) is obliged to disclose the knowledge or suspicion to an STRO officer. "Criminal conduct" includes the 335 predicate offences for money laundering as well as the terrorist financing offences. The MAS Notices specify that attempted transactions must also be reported. There are comprehensive "safe harbor" provisions for STR reporting. Tipping off is also prohibited, although the criminal offence only applies to a transaction that has already been reported and not specifically to those in the process of being reported. The rate of STR reporting has been increasing, with financial institutions filing over 6 000 STRs in 2007 (up to 14 November).

17. Requirements for internal AML/CFT controls, including compliance management arrangements with a compliance officer at the management level, internal audit, training, and screening of employees are being implemented effectively in the various financial sectors. Financial institutions (other than commodities futures brokers) implement their requirements for group AML/CFT policies. These require that overseas branches or subsidiaries apply the higher of the two AML/CFT standards where they differ, and report to MAS when this is not possible due to domestic law. Singapore implements comprehensive requirements concerning shell banks.

18. The MAS is Singapore's central bank and financial services regulator. It has supervisory responsibility over banks, finance companies, merchant banks, insurance companies, capital markets services (CMS) licensees, financial advisers, moneychangers and remittance agents. From early 2008, MAS will also have regulatory oversight of commodity futures trading in Singapore. MAS sets its own budget (about half of which is spent on supervision) and hires the staff it requires to perform its supervisory functions.

19. Financial institutions have to obtain MAS' approval to carry on business in Singapore. MAS' approval is generally required for: (1) the appointment of directors and senior management and in the case of institutions carrying out the banking business, nominating committees; and (2) specific

threshold changes in shareholdings of the financial institution. The directors and some members of senior management of financial institutions that are subject to the Core Principles are required to satisfy fit and proper criteria. Money changing and remittance (value transfer) businesses also require a license from MAS in order to legally operate. The Singapore authorities have made some efforts to locate unlicensed remitters and sanction them accordingly. However, Singapore should develop more pro-active policies with a view to reducing the number of possible unlicensed money-changing and remittance businesses considering the large communities of migrant workers from countries with poor banking systems present in Singapore.

20. MAS uses a risk-based approach to financial supervision. Each institution is assessed and assigned two ratings: (1) an impact rating that assesses the potential impact which it might have on Singapore's financial system, economy and reputation in the event of a significant mishap (*e.g.* financial or major control failure, and prolonged business disruption); and (2) a risk rating which assesses the likelihood of these significant mishaps occurring. It then uses a risk assessment, CRAFT (Common Risk Assessment Framework and Techniques), to evaluate the risk of an institution. Finally, the MAS determines the appropriate supervisory strategies and, in turn, the level of supervisory intensity required. Impact and risk ratings are combined to assign the institution to one of four categories ("buckets") of supervisory significance. The intensity of supervision varies according to the bucket.

21. For financial institutions that are subject to the Core Principles (*i.e.* banks, merchant banks, finance companies, financial advisers, CMS licensees and insurers), MAS applies similar supervisory measures used for prudential purposes in relation to AML/CFT.

22. MAS has a broad range of powers to monitor and ensure that financial institutions comply with AML/CFT measures, including powers of off-site surveillance, auditing and on-site visits and inspections. MAS conducts both routine and thematic on-site inspections of the financial institutions under its supervision. All financial institutions are subjected to base-level supervision and monitoring. The scope and frequency of inspection varies among the financial institutions, depending on MAS' impact and risk assessment on the financial institutions. The inspection period for each financial institution could range from 2-3 days for institutions like financial advisers to 1-4 weeks for banks, depending on the size of the financial institution and the scope of inspection. For 2007 (up to 14 November), MAS carried out 27 on-site inspections of banks (which included AML/CFT), among them five thematic AML inspections (*i.e.* AML/CFT only). The scope of MAS inspection includes a review of the financial institutions' policies and procedures, books and records, and sample or transaction testing. MAS also has comprehensive powers to require a financial institution to produce its books, accounts and documents, and to afford MAS access to such information or facilities as may be required to conduct the inspection or investigation.

23. Financial institutions that fail to comply with or properly implement their AML/CFT obligations are subject to a range of criminal, regulatory and supervisory measures. Additionally, a director, managing director, and a varying range of management personnel and, in some cases, officers of the financial institution may be personally liable if they fail to take all reasonable steps to secure the financial institution's compliance with relevant legislation and for non-compliance with directions issued to specific institutions pursuant to the MAS Act. MAS may also direct the removal of a chief executive or officer, or issue him/her a formal reprimand.

24. The MAS Act authorises the MAS to notify a financial institution or make any recommendation that it sees fit. This broad power thus includes the ability to issue a warning or reprimand letter, which could indicate specific deficiencies that need to be rectified, order a change in management, suspend or withdraw a license, or issue a fine. Recent amendments to the MAS Act create a derivative liability in the MAS Act on officers (directors, members of the committee of management, chief executive, manager, secretary or other similar officers) where non-compliance by a financial institution is attributable to their consent, connivance or neglect.

25. MAS reports that administrative sanctions such as a letter of reprimand or letter requiring remedial action have been very effective in getting financial institutions to rectify their breaches and deficiencies. No criminal sanctions have been issued; fines have only been issued against money remitters and bureaux de change.

4. Preventive Measures – Designated Non-Financial Businesses and Professions (DNFBPs)

26. Singapore has applied AML/CFT preventive measures to trust companies (that are regulated as financial institutions) and lawyers. Singapore has not yet applied preventive measures to accountants when they undertake the type of work covered by Recommendation 12, trust service providers (other than trust companies and lawyers), company service providers, dealers in precious metals and stones and real estate agents. Physical casinos are not yet in operation, and internet casinos are prohibited.

27. Lawyers are subject to the Legal Profession (Professional Conduct) Rules (the 'Rules') issued by the Law Society. Amendments to the Rules with respect to some CDD and record keeping requirements came into operation on 15 August 2007. The Council of the Law Society has also issued a Practice Direction on AML/CFT that came into force on 15 August 2007. It sets out more details and complements the obligations under the Rules. For example, lawyers are required to take reasonable measures to ascertain the identity of a client before accepting instructions on any matter. Lawyers must obtain satisfactory evidence as to the nature and purpose of the business relationship with the client when carrying out activities of most of the types covered by Recommendation 12 for a client and they must examine the background and purpose of transactions that are complex, unusual or large. However, there are still key deficiencies in the Practice Direction in that there are no specific requirements, for example, for a lawyer to identify the beneficial owner for all customers or to determine if the customer is acting on behalf of another person, or conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

28. The reporting requirements that apply to financial institutions under the CDSA (s.39) and TSOFA (s.8 and 10) apply to all persons, and therefore to all DNFBPs. The safe harbor and no tipping off provisions also apply. However, there are some concerns about how effectively the reporting requirement has been implemented in the DNFBP sectors.

29. There are currently no enforceable obligations relating to Recommendations 15 and 21 in relation to DNFBPs, other than lawyers and trust companies that are regulated as financial institutions.

30. Lawyers are supervised for compliance with AML/CFT requirements by their SRO; however, as the regime is very new, its effectiveness cannot yet be assessed. Real estate agents, dealers in precious metals and stones, and TCSPs (other than trust companies that are regulated as financial institutions as described in section 3 of this report) have not been issued with AML/CFT measures (other than the reporting obligations) and are therefore not monitored for AML/CFT compliance.

5. Legal Persons and Arrangements & Non-Profit Organisations

31. ACRA is the central registration authority in Singapore for business entities. ACRA maintains a register containing information on entities, including ownership and control of companies and limited liability partnerships. Supplementing this information is a requirement for entities to maintain information on their premises (such as shareholder registers) which may be, in some instances, available for public inspection. While the investigative powers are generally sound and widely used, there are limited measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons which can be obtained or accessed in a timely fashion by competent authorities.

32. The competent authorities have powers to access information on the beneficial ownership of trusts. However, availability of that information is limited by the fact that only trusts administered by trustee companies and trust company service providers are obliged to maintain such information.

33. Singapore's non-profit organisation (NPO) sector is significantly populated by two forms of entities, namely charities and Institutions of a Public Character (IPCs). Charities are established exclusively for charitable objects including relief of poverty, advancement of education, advancement of religion and other purposes beneficial to the community. IPCs are NPOs whose activities are beneficial to the community in Singapore as a whole and are authorized to receive tax-deductible donations. All charities and IPCs in Singapore are supervised by the Commissioner of Charities who is assisted by six other government agencies overseeing charities and IPCs in their respective sectors. The Commissioner of Charities has conducted outreach to the NPO sector concerning Singapore's AML/CFT laws; how to counter certain ML/FT risks within the sector; and reminding NPOs of their obligations to file STRs. No charity or IPC has yet filed a STR. All charities and IPCs in Singapore are subject to some form of supervision by the Ministry of Community Development, Youth and Sports. The Commissioner of Charities also has the power to sanction violations of oversight measures. Charities must keep accounting records sufficient to show and explain all the charity's transactions monies received and expended and a record of assets and liabilities.

6. National and International Co-operation

34. Singapore utilises a multi-agency AML/CFT strategy involving law enforcement, policy makers, regulators and the private sector. This effort is led by a high-level Steering Committee established in 1999. The Steering Committee is supported by the working-level Inter-Agency Committee (IAC) comprised of 15 agencies and departments. To ensure a coordinated effort in combating terrorism (including terrorist financing), members of the IAC are also represented on the Inter-Ministry Committee on Terrorism (IMC on Terrorism) which was established in 2001.

35. Singapore is a party to the Vienna Convention, the FT Convention, and the Palermo Convention.

36. The Mutual Assistance in Criminal Matters Act (MACMA) allows Singapore to provide mutual legal assistance (MLA) to other jurisdictions, in relation to criminal investigations or criminal proceedings for offences that are covered under the Act (335 crimes, including ML and FT). Requests for MLA are processed by the Attorney General's Chambers (AGC). Amendments to the Act in April 2006 mean that a mutual legal assistance treaty (MLAT) is no longer required before coercive assistance can be provided to any requesting State as long as the requesting State provides a reciprocity undertaking before assistance is granted. With respect to MLATs, Singapore has bilateral MLATs with the Hong Kong Special Administrative Region, India, the United States (in the form of a Drug Designation Agreement) and a MLAT relationship with Malaysia, Vietnam, Brunei Darussalam, and Laos. Dual criminality is required for coercive measures, but is not interpreted in an overly strict manner as it is the criminal conduct alleged which is examined as a whole to determine whether the conduct would amount to a scheduled offence in the CDSA list in Singapore, not the label of the offence or its constituent elements. Assistance that may be provided includes the production or seizure of information, documents, or evidence (including financial records) from financial institutions, other entities, or natural persons; and searches of financial institutions, other entities, and domiciles. The 2006 MACMA legislation appears to have addressed some major deficiencies in mutual legal assistance previously encountered in foreign requests to Singapore for assistance. Singapore authorities maintain that MACMA has enabled them to provide MLA in a timely, constructive and effective manner. However, there has not been sufficient time to show whether the provisions are working fully effectively.

37. Singapore may provide assistance to foreign governments in the enforcement of a foreign confiscation order or the restraining of dealing in any property that is related to that confiscation order and is reasonably believed to be located in Singapore, as ancillary to a foreign criminal prosecution. MACMA also authorises Singapore to enforce foreign instrumentalities orders; however this does not

cover instrumentalities intended for use in the commission of offences or substitute property. Singapore authorities indicate that other legislation could be used for these items; however, the effectiveness of those provisions cannot be assessed.

38. ML is an extraditable offence as it is listed in the First Schedule to the Extradition Act. Likewise, FT offences are deemed extraditable crimes under the Extradition Act by virtue of section 33(1) of the TSOFA. Singapore can extradite its own nationals.

39. Singapore has also implemented measures to facilitate administrative cooperation between domestic authorities and foreign counterparts outside of the formal MLA process.

7. Resources and Statistics

40. Singapore has dedicated appropriate financial, human, and technical resources to the various areas of its AML/CFT regime. All competent authorities are required to maintain high professional standards, including standards concerning confidentiality, and receive adequate AML/CFT Training.

41. Singapore generally maintains comprehensive statistics, enabling it to assess the effectiveness of its AML/CFT measures. However, the statistics relating to the number of cases and amounts of property frozen, seized and confiscated do not specifically distinguish between cases in which there is a close relation between the domestic predicate offences and the money laundering investigations.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General Information on Singapore

1. Singapore is located in Southeast Asia, just south of the Malaysian peninsula. An island-state, Singapore occupies a land area of approximately 700 square kilometres. The population of Singapore stands at 4.5 million, of which 3.6 million are Singapore citizens and permanent residents. The remaining 0.9 million are non-residents on long term passes who are working, studying or living in Singapore. A multi-racial and multi-religious society, the three largest ethnic groups are the Chinese, the Malays and the Indians.

Economy

2. Singapore has enjoyed high, stable economic growth since achieving independence. In 2006, GDP growth was at 7.9%, largely led by the manufacturing, wholesale & retail and financial services sectors. Among the industries that have seen considerable expansion are biomedical production, transport engineering and financial services. Singapore was ranked fourth in the 2007 City of London's Global Financial Centres Index. The financial sector accounts for about 11% of GDP. About 480 licensed international financial institutions have a presence in Singapore. There are three main local banks: DBS Bank, the United Overseas Bank (UOB), and the Overseas-Chinese Banking Corporation (OCBC). Singapore has a very significant private banking and assets management sector, with a large number of overseas clients. As well, Singapore is a major destination point for international equity and direct foreign investment. Numerous reputable, international financial institutions have a presence in Singapore.

System of government

3. A sovereign state since 1965, Singapore is a republic operating on a Westminster system of unicameral parliamentary government. Parliament is elected by general election every five years. The Singapore Parliament consists of both elected and non-elected Members of Parliament (MPs). Elected MPs are drawn from candidates who have won the general elections, while non-elected MPs are appointed by Parliament and may be non-politicians nominated to provide a greater variety of non-partisan views. The Cabinet, chaired by the Prime Minister, is collectively responsible to the Parliament. Singapore has also put into place a system of Elected President whose duty is to safeguard the national reserves accumulated by previous terms of Governments and to preserve the integrity of the public services. The President is non-executive, and is directly elected by the people for a 6-year term.

Legal system and hierarchy of laws

4. The judiciary is one of the three constitutional pillars of government along with the legislature and the executive. The judiciary's function is to independently administer justice. The judiciary comprises the Supreme Court (the Court of Appeal and High Court) and the Subordinate Courts (Magistrate and District Courts). The highest court is the Court of Appeal, which hears both civil and criminal appeals from the High Court and the subordinate courts. Singapore has a common law legal system. Decisions of the Court of Appeal are binding on lower courts.

5. The Singapore regulatory structure utilises various enforceable means, such as laws ("Acts"), Regulations, and Notices. Regulations, Orders, Declarations, and Notifications are issued under the authority of the respective parent Act and provide greater detail to statutory obligations. Regulations are published in the Government Gazette and have the force of law. Some provide for criminal offences.

Transparency, good governance, ethics and measures against corruption

6. In general, the domestic crime rate (*i.e.* level of offending) is low in Singapore which is largely attributable to the deterrent effect of stringent and effective law enforcement. According to Singapore authorities, domestic corruption is minimal. The Corrupt Practices Investigation Bureau (CPIB), which has been in operation since the 1950s, is an independent body that investigates and aims to prevent corruption in the public and private sectors in Singapore. The CPIB enforces the Prevention of Corruption Act (PCA), Chapter 241. Offenders found guilty of corruption offences are liable to a fine not exceeding SGD 100,000 and/or imprisonment for a term that may extend to seven years. On conviction a court shall order the offender to pay a penalty equal to the amount received, see sections (ss.) 7 and 10-12, PCA.

7. Singapore has consistently ranked in the top five nations in Transparency International's (TI's) Corruption Perception Index, In the recently released 2007 TI report, Singapore ranked 4 out of 179 countries, where 1st is the least corrupt. Also in TI's 2006 Global Corruption Barometer report, Singapore had the highest percentage ranking among respondents who ranked their government's fight against corruption (89% effective). In the same TI report, Singapore's police, legal system and Parliament scored among the lowest in the world in relation to the impact of corruption on different sectors. Singapore signed the United Nations Convention against Corruption on 11 November 2005, but has not yet ratified it due to domestic measures that need to be implemented prior to ratification. Singapore is in the process of implementing those measures after which it will be in a position to ratify this Convention.

1.2 General Situation of Money Laundering and Financing of Terrorism

8. As a developed, open and stable economy located in South East Asia, Singapore faces a range of money laundering and terrorist financing risks. Nevertheless, Singapore adopts a tough position towards all forms of criminal activity. Singaporean authorities emphasise that the level of domestic crime in Singapore is very low. However, there exist significant risks from money laundering proceeds of crime generated across the region. There are risks from capital flight associated with corruption in other South East Asian countries, as well as the proceeds of crime from a range of other offences, as highlighted by typologies reports, press articles and international studies. Singapore's position as the most stable and prominent financial centre in SE Asia, coupled with the regional history of trans-national organised crime, large-scale corruption in neighbouring states and a range of other predicate offences in those states increase the risks that Singapore is an attractive destination for criminals to attempt to launder their criminal proceeds.

9. The size and growth of Singapore's private banking and assets management sector could pose a significant money laundering risk based on known typologies. In 2006, the assets managed by Singapore-based managers grew by 24% to SGD 891 billion (approximately USD 581 billion). Many assets belong to overseas-based clients, 50% of whom are non institutional, including 43% from the Asia Pacific region (excluding North America) and from jurisdictions with relatively low levels of AML/CFT compliance. For instance, of the total assets held in this section, SGD 180 billion (USD 115 billion) is from non-institutional clients in the Asia/Pacific region (excluding North America). In addition, Singapore is a major destination point for international equity and direct foreign investment, and international visitors, with a total of SGD 298 billion and SGD 311 billion invested respectively in 2006.

10. Regionally, there are key risks of cash couriers, trade based money laundering, underground banking and use of the formal banking sector to facilitate money laundering. APG Typologies reports indicate a range of typologies by which money launderers target Singapore's stable financial sector to launder funds in the region. Australia, for example, reported fund flows associated with illegal activity in Australia utilising Singapore financial service providers as a transit point for funds that are ultimately destined for other parts of Asia.

11. There are vulnerabilities from cash couriers seeking to physically move funds to Singapore to place in the stable financial sector, as highlighted by regional typologies. There are 10 million visitors per year to Singapore, with 2 million visitors from Indonesia. In 2006, for instance, there were 9.7 million visitors to Singapore of which Indonesians accounted for 20%. The People's Republic of China was the second largest source with 10% of visitors. Australia, India, Malaysia and Japan are other major sources of visitors.

12. Singapore has taken a number of initiatives to mitigate the risk of regional and international money laundering. In April 2006, the Mutual Assistance in Criminal Matters Act (MACMA) was amended to allow assistance to be provided to any requesting country in the absence of a MLAT, provided that the requesting country gives an undertaking of reciprocity in relation to a future similar request from Singapore. Accordingly, a mutual legal assistance treaty is no longer a pre-requisite for the provision of legal assistance to any country. Singapore has also signed the 2004 regional Treaty on Mutual Legal Assistance. Singapore, Malaysia, Vietnam, Laos and Brunei Darussalam have since ratified this Treaty. In addition, the Financial Intelligence Unit, STRO, has signed Memoranda of Understanding (MOUs) with the FIUs from 11 countries/jurisdictions, although most of these involve countries outside of Singapore's immediate South East Asia geographic region.

13. Singapore adopts a tough position towards all forms of criminal activity, and has a low domestic crime rate. The heavy penalties for drug trafficking offences has also kept Singapore safe from the regional threat and there are no areas in which drugs can be purchased easily or openly. Nevertheless, statistics indicate that there could be some incidents of domestic crime that may potentially generate significant proceeds of crime, including drug trafficking, cheating (which includes fraud), criminal breach of trust, forgery and counterfeiting of currency, as indicated in the chart below. It was explained by the authorities that the overwhelming majority of the cases do not involve significant amounts of criminal proceeds and could include instances of petty thefts, etc.

Conviction rates for predicate offences

Predicate offence	2004	2005	2006
Cheating	412	389	322
Criminal Breach of Trust	521	568	508
Forgery	93	73	55
Counterfeiting of currency	0	4	23
Falsification of Accounts	5	12	13
Drug trafficking	484	403	578*

* Some of these cases are pending.

14. A further concern is that Singapore's stable financial sector creates a risk that criminals may abuse the system by attempting to "legitimise" the proceeds of crime, including proceeds generated by offences committed abroad.

15. Singapore authorities indicate that elimination of domestic crimes of unlicensed money lending and illegal gambling is a priority. Pursuant to its analysis and investigations, STRO has disseminated information obtained from STRs on over 900 entities relating to unlicensed money lending and 250 entities relating to illegal gambling to the enforcement agencies.

16. Since 2005, STRO has also observed an emerging trend whereby account holders who have satisfied the Customer Due Diligence (CDD) requirements are recruited as transaction managers or "money mules" to assist in the transfer of illegally obtained funds, frequently through phishing or other internet fraud. These money mules generally retain a commission of between 3 – 5% of the funds transferred (into their accounts) before the onward transfer of the funds. As at 14 November 2007, STRO has disseminated over 100 STRs relating to money mules, which has led to 9 money laundering investigations into 77 entities. In total, SGD 59 000 in proceeds of crime were identified and/or surrendered. Investigations further revealed that more than SGD 1.7 million has been

transferred through money mules in Singapore. It is likely that this amount will grow in the future given the increasing occurrences of phishing scams worldwide.[3]

17. Singaporean authorities also identify vulnerabilities in the securities and futures sector, and have taken proactive action to address them. The proactive action includes conducting outreach sessions, holding dialogues and consultations with the industry, performing AML/CFT focused on-site examination and off-site supervision, and developing an AML/CFT self-assessment framework.

18. Singaporean authorities have also highlighted risks from terrorist groups and terrorist financing. A number of terrorist organisations have tried to operate on Singaporean territory. The authorities have taken concerted action against Jemaah Islamiyah and its members and have identified and frozen terrorist assets held in Singapore. Singapore continues to actively monitor for potential terrorism-related activities that may occur in Singapore and is alert to the potential threat posed by self-radicalised individuals who are not recruited by or the member of any terrorist organisation, but who nonetheless subscribe to jihadist ideology. Following a security operation that commenced in December 2001, Singapore has dismantled the local Jemaah Islamiyah (JI) terrorist network and has confirmed that the network is no longer carrying out its activities in Singapore and that the amount of terrorist funds held in Singapore was small.

1.3 Overview of the Financial Sector and DNFBP

a. Overview of Singapore's financial sector

19. Singapore is a major financial centre in Asia. As of 14 November 2007, there were more than 500 local and foreign financial institutions in Singapore (see table below). Financial services accounted for 11% of Singapore's GDP and 5% of total employment in the economy.

Type of institution	Number of financial institutions as of 14 November 2007
Banks (total):	**161**
Commercial banks (total):	112
Local banks	6
Foreign banks (total): *Foreign full banks* *Wholesale banks* *Offshore banks*	106 *24* *39* *43*
Merchant banks	49
Finance Companies	**3**
Capital Markets Services Licensees	**197**
Financial Advisers & Insurance Intermediaries	**133**
Life insurers	**17**
Trust companies	**36**
Money exchangers	**379**
Money remitters	**91**

20. Singapore has a total of 112 commercial banks with assets of SGD 1 363 billion. There are also 49 merchant banks, with assets of SGD 78 billion. In addition, three finance companies (with total assets of approximately SGD 10 billion) operate in Singapore, focusing on small-scale financing including instalment credit for motor vehicles and mortgage loans for housing.

21. There are 197 capital markets services licensees performing a variety of dealing and trading, advising on corporate finance, fund management and providing custodial services for securities, and 133 financial advisers and insurance brokers. Assets under management total approximately

[3] At the time of the on-site visit, the exchange rate was approximately SGD 1 = 0.48174 Euros / 0.65828 United States dollars.

SGD 1 113 billion. The two approved exchanges are the Singapore Exchange Securities Trading Limited (SGX-ST), which operates the securities market and the Singapore Exchange Derivatives Trading Limited (SGX-DT) which operates the futures market. As at 31 March 2007, 715 companies are listed on SGX-ST with a total market capitalisation of SGD 662 billion.

22. There are 17 life insurers. As at the end of 2006, total in force annual premiums for the life insurance industry amounted to SGD 6.7 billion, while total new single premiums and annuities amounted to SGD 6.9 billion and SGD 0.4 billion respectively. As at 14 November 2007, there were 36 licensed trust companies in Singapore, with total assets of approximately SGD 113 billion. Additionally, there are also 470 licensed money-changers and remittance agents currently operating. [4]

23. The types of financial institutions that are authorized to carry out the financial activities listed in the Glossary of the FATF 40 Recommendations are summarized in the following table.

TYPES OF FINANCIAL INSTITUTIONS CARRYING OUT FINANCIAL ACTIVITIES IN SINGAPORE	
Financial Activity (as defined in Glossary to FATF 40 Recommendations)	***Categories of Financial Institutions performing such activity in Singapore***
1. Acceptance of deposits and other repayable funds from the public	Banks Merchant Banks Finance companies
2. Lending	Banks Merchant Banks Finance companies Licensed or exempt moneylenders that grant loans to the general public under the Moneylenders Act
3. Financial leasing	Banks
4. Transfer of money or value	Banks Holders of remittance business licensed under the Money-Changing and Remittance Businesses Act
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Banks Credit Card Issuers licensed under the MAS Act
6. Financial guarantees and commitments	Banks Merchant Banks Finance companies
7. Trading in: - money market instruments - foreign exchange - exchange, interest rate and index instruments - transferable securities - commodity futures trading	Banks Merchant Banks Holders of capital markets services licence under the Securities and Futures Act Commodity futures brokers licensed under the Commodity Trading Act
8. Participation in securities issues and the provision of financial services related to such issues	Banks Merchant Banks Holders of capital markets services licence Holders of financial adviser's licence under the Financial Advisers Act
9. Individual and collective portfolio management	Banks Merchant Banks Holders of capital markets services licence
10. Safekeeping and administration of cash or liquid securities on behalf of other persons	Banks Merchant Banks Holders of capital markets services licence CIS approved trustees under the Securities and Futures Act
11. Otherwise investing, administering or managing finds or money on behalf of other persons	Banks Merchant Banks Holders of capital markets services licence Holders of financial adviser's licence

[4] For paras 20 – 22, the asset figures are as of 31 Dec 2006.

TYPES OF FINANCIAL INSTITUTIONS CARRYING OUT FINANCIAL ACTIVITIES IN SINGAPORE	
Financial Activity (as defined in Glossary to FATF 40 Recommendations)	***Categories of Financial Institutions performing such activity in Singapore***
12. Underwriting and placement of life insurance and other investment related insurance	Banks Merchant Banks Life insurers licensed under the Insurance Act
13. Money and currency changing	Banks Merchant Banks Money-changers licensed under the Money-Changing and Remittance Businesses Act

b. Overview of designated non-financial businesses and professions (DNFBPs)

24. ***Casinos:*** The Casino Control Act (CCA) was enacted in February 2006 and permits licensed casinos to operate in Singapore. The first casinos will open in 2009. Internet casinos are prohibited.

25. ***Real estate agents:*** There are 1 629 licensed estate agencies in Singapore. Only estate agencies are licensed, not individual agents.

26. ***Lawyers:*** As of 2006, there were 806 legal firms and 3 476 legal practitioners with practicing certificates in Singapore.

27. ***Public accountants/ auditors:*** There are 800 accountants working in accounting firms, accounting corporations or accounting limited liability partnerships providing public accountancy services (*i.e.* the audit and reporting on financial statements and the doing of such other acts that are required by written law to be done by a public accountant). While only a person registered as a public accountant under the Accountants Act may call and hold him or herself to be a "public accountant", the use of the title of "accountant" is otherwise not regulated by statute.

28. ***Dealers in precious metals and precious stones:*** There are more than 700 jewellery retailers in Singapore, with a combined turnover of about SGD 1.1 billion a year.

29. ***Trust and company service providers (TCSP):*** There are 36 trust companies in Singapore, which are licensed to provide a range of fiduciary services, including establishing and administering trusts. Lawyers, trustee-managers and trustees/administrators of business trusts may also provide trust services. Company service providers are not specifically regulated by statute. However, only persons prescribed by law (*e.g.* lawyers, accountants, corporate secretarial agents, members of the Singapore Association of the Institute of Chartered Secretaries and Administrators, and members of other prescribed professional associations) may file documents on behalf of a third party. Approximately 2 200 professionals have been authorised to undertake this activity.

1.4 Overview of Commercial Laws and Mechanisms Governing Legal Persons and Arrangements

30. There are three primary business entities in Singapore each governed by separate statutory regimes:

Business Entities	Governing Statutes
• Company	• Companies Act (CA)
• Limited liability partnership	• Limited Liability Partnership Act (LLPA)
• Sole proprietor	• Business Registration Act (BRA)

31. ***Companies:*** Singapore companies are incorporated pursuant to Chapter 50 of the CA and have separate legal personality. The CA regulates the establishment, maintenance and dissolution of companies. A company may be: (1) limited by shares, (2) limited by guarantee, or (3) an unlimited

company. The vast majority of companies in Singapore fall into the first category of which there are three kinds:

(a) Private companies (172 885 registered): up to 50 shareholders with restricted share transfers rights.

(b) Public companies (2 034 registered): more than 50 shareholders which may offer shares and/or debentures to the public.

(c) Foreign companies (1 996 registered): overseas established companies registered to conduct business in Singapore and with a branch in Singapore.

32. Foreign companies (defined to include limited liability partnerships) are companies that are incorporated outside Singapore, but conduct business in Singapore.

33. ***Limited Liability Partnerships*** *(3 745 registered):* A limited liability partnership (LLP) is a body corporate with separate legal personality from its partners and perpetual succession (s.4 LLPA). A "partner" is any person (including a body corporate) who is admitted as a partner in accordance with a limited liability partnership agreement. Changes in specific partners of a LLP do not affect the existence, rights or liabilities of the partnership as a separate entity. A LLP combines the benefits of a partnership with those of private limited companies.

34. ***Sole proprietorships*** *(112 004 registered)*: A sole proprietorship is owned by one person or a locally incorporated company and, in contrast to companies and LLPs, there is no legal distinction between a business entity as a sole proprietorship and the owner (*i.e.* it cannot sue or be sued in its own name and it cannot own or hold any property). As there is no limitation on liability, the owner is responsible for all debts and other liabilities of the business. Sole proprietorships are not legal entities or legal persons.

35. ***Trusts:*** Singapore inherited a British common law legal system which recognises a wide range of trusts, including express, discretionary, implied, and many other forms of trusts. The Trustee Act provides the basic legal framework for trusts in Singapore; however, as with all common law jurisdictions, case law is also relevant to trust legal issues. There is limited information on the number of trusts that have been formed or are administered in Singapore.

1.5 Overview of Strategy to Prevent Money Laundering and Terrorist Financing

a. AML/CFT Strategies and Priorities

36. Singapore has adopted a multi-pronged systems approach to responding to ML/TF risks. AML/CFT efforts are centred on having a sound and comprehensive legal, institutional, policy and supervisory framework, low domestic crime rate, intolerance for domestic corruption, an efficient judiciary, and a long established culture of compliance and effective monitoring of the measures implemented. Singapore authorities indicate that they have also taken a proactive stance in tracking down and disrupting terrorist movements by sharing intelligence with other jurisdictions. The authorities identify the key elements of Singapore's overall strategy in combating money laundering and terrorist financing to be as follows:

(a) Identifying areas of high priority for action based on the risk assessment of the major threats and vulnerabilities in respect of money laundering and terrorist financing.

(b) Implementing international standards rigorously, in particular, the FATF 40+9 Recommendations.

(c) Maintaining a strong penal regime against drug trafficking, terrorism and other serious crimes.

(d) Having effective law enforcement that serves as a strong deterrent.

(e) Imposing a strict selection criteria for financial institutions seeking admission to Singapore's financial sector.

(f) Ensuring effective supervision of financial institutions operating in Singapore.

(g) Hiring motivated and professional staff to develop and implement AML/CFT policies and measures.

(h) Implementing a high level of co-ordination and co-operation across government agencies.

(i) Providing assistance to a number of other jurisdictions through formal and informal channels, including the sharing of information and intelligence.

37. Singapore intends to better strengthen its AML/CFT regime by paying more attention to the designated non-financial professions and businesses that are susceptible to money laundering risks. The new initiatives include:

(a) Issuing AML regulations for casino operators and junket promoters.

(b) Implementing a declaration system for incoming and outgoing travellers for detection of cross-border transportation of currency or bearer negotiable instruments.

(c) Extending the AML/CFT requirements to Commodities Futures Brokers in early 2008.

(d) Extending outreach programmes to the DNFPB sector including lawyers, real estate agents, jewellers and businesses in general (through ACRA).

(e) Drafting Practice Directions by the Law Society of Singapore.

(f) Studying the possibility of a more detailed framework for AML regulations to be applied to company service providers.

(g) Reviewing the Corruption, Drug Trafficking and other Serious Crimes Act to fine-tune the relevant provisions, taking into consideration market feedback on implementation issues.

38. Additionally, the elimination of unlicensed money lending and illegal gambling activities are priorities for the Singapore government.

b. The institutional framework for combating money laundering and terrorist financing

(i) Ministries and co-ordinating committees

39. ***Steering Committee (SC):*** In 1999, Singapore established a high-level Steering Committee, comprised of the Permanent Secretary of the Ministry of Home Affairs [PS (HA)], Permanent Secretary of the Ministry of Finance [PS (F)] and Managing Director of the Monetary Authority of Singapore, to determine broad policy objectives for combating money laundering and terrorist financing. This Committee leads the national effort to develop and implement Singapore's AML/CFT regime.

40. ***Inter-Agency Committee:*** The Steering Committee is supported by a multi-agency working group, the Inter-Agency Committee (IAC), comprised of the various agencies that play an AML/CFT role. Representatives of these agencies meet several times a year. The IAC makes recommendations to the SC for decision or guidance. For major policy changes that require political endorsement, the SC tables the issues at Cabinet meetings.

41. ***Inter-Ministry Task Force on Anti-Terrorism:*** Members of the IAC are also represented on the Inter-Ministry Task Force on Anti-Terrorism. This Task Force was set up in 2001 under the auspices of the Attorney-General's Chambers and the Ministries of Foreign Affairs and Law to ensure Singapore's full compliance with international obligations and to strengthen its national capacity to implement measures to combat international terrorism.

42. ***Ministry of Home Affairs (MHA):*** The MHA is responsible for maintaining law and order, and internal security. MHA oversees the various law enforcement agencies, including the Singapore Police Force (SPF) and its Commercial Affairs Department (CAD), which includes the FIU – the Suspicious Transaction Reporting office (STRO) – and the Central Narcotics Bureau (CNB). The MHA has responsibility for the relevant AML/CFT legislation, namely the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and the Terrorism (Suppression of Financing) Act.

43. ***Ministry of Law (MinLaw):*** The MinLaw is responsible for constitutional law and trustee matters, legal policies on civil and criminal justice, alternative dispute resolution and community mediation, the administration of intellectual property rights, as well as the administration of land titles and the management of state properties. MinLaw is also responsible for the Mutual Assistance in Criminal Matters Act (MACMA), the Extradition Act and the United Nations Act.

44. ***Attorney-General's Chambers (AGC):*** The AGC is an independent Organ of State responsible for legislative drafting and reform; advising the Government on all domestic and international legal matters; prosecution of offenders; making applications to prevent dissipation of proceeds of crime; and processing requests for mutual legal assistance and extradition. It also provides legal advice to government departments and law enforcement agencies on the interpretation of AML/CFT laws and issues. The AGC's Deputy Public Prosecutors (DPPs) prosecute ML and FT offences as well as most of the serious offences listed in the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA). Requests for mutual legal assistance in criminal matters and extradition are processed by the AGC, whose officers also lead or assist in the negotiations of mutual legal assistance and extradition treaties

45. ***Ministry of Finance (MOF):*** MOF is the central ministry that is responsible for the fiscal policies including revenue and tax collection, budgeting and expenditure of the government. The main regulatory statutes under the MOF are the Companies Act, Business Registration Act and Accountants Act. MOF is the parent ministry to the Inland Revenue Authority of Singapore (IRAS), the Accounting and Corporate Regulatory Authority (ACRA) and the Singapore Totalisator Board. It also has the Accountant-General's Office, the Singapore Customs and Centre for Shares Services – Vital.Org as its departments.

(ii) Criminal justice and operational agencies

46. ***Commercial Affairs Department (CAD):*** CAD's Financial Investigation Division (FID) is tasked to investigate the money laundering of benefits derived from drug trafficking and serious crimes, terrorism financing and other offences under the CDSA and the Terrorism (Suppression of Financing) Act (TSOFA). FID is comprised of three branches – namely, the Financial Investigation Branch (FIB), the Proceeds of Crime Unit (PCU), and the Suspicious Transaction Reporting Office (STRO):

- FIB investigates money laundering and terrorism financing.

- PCU identifies and seizes assets which represent criminal proceeds and works with FIB. PCU conducts asset-tracing investigations to identify and seize hidden criminal proceeds, and also handles the subsequent confiscation and disposal of seized assets.

- STRO is Singapore's FIU and acts as the main agency for receiving and analysing suspicious transaction reports (STRs). STRO is also involved in negotiating memorandum of understanding (MOUs) with foreign FIUs for the exchange of financial transaction information, and organising outreach programs to the financial and non-financial sectors to increase awareness on ML and FT.

47. ***Central Narcotics Bureau (CNB):*** The CNB is responsible for enforcing the CDSA, in relation to the seizure of drug assets. CNB's Financial Investigation Division investigates the financial affairs of drug traffickers with a view to confiscating all benefits derived from drug trafficking. CNB also handles CAD's screening requests and deals with extradition matters of drug offenders.

48. ***Corrupt Practices Investigation Bureau (CPIB):*** The CPIB is a department within the Prime Minister's Office and is responsible for enforcing the CDSA, in relation to corruption.

49. ***Suspicious Transaction Reporting office (STRO):*** STRO is Singapore's financial intelligence unit (FIU).

50. ***Immigration & Checkpoints Authority (ICA):*** The ICA is the immigration control and border enforcement authority responsible for implementing Singapore's declaration and disclosure system and the border.

(iii) Financial sector bodies – government

51. ***Monetary Authority of Singapore (MAS):*** The MAS is Singapore's central bank and financial services regulator. As an integrated regulator, it has supervisory responsibility over banks, finance companies, merchant banks, insurance companies, capital markets services licensees, financial advisers, moneychangers and remittance agents. At a broad policy level, it participates in the formulation of legislative and administrative measures to combat ML/FT and has issued and updated notices to financial institutions requiring them to take appropriate AML/CFT preventative measures.

(iv) Financial sector bodies – associations

52. ***Association of Banks in Singapore (ABS):*** The ABS comprises a wide spectrum of banking entities ranging from major global banks to smaller financial niche service providers. Currently, there are 110 ordinary members (*i.e.* full, qualifying full, wholesale or offshore banks licensed by MAS) and eight associate members (*i.e.* representative offices of foreign banks that do not conduct any banking business in Singapore). ABS represents and furthers the interest of its member banks, sets standards of good practice and promotes continuous upgrading of expertise among their employees.

53. ***Life Insurance Association of Singapore (LIA):*** Members of the LIA are either licensed life insurance corporations ("ordinary members") or licensed reinsurance corporations ("associate members"). Comprising 14 ordinary members and three associate members, the LIA's objectives are to develop the life insurance business in Singapore, advocate good industry practices and promote public awareness of life insurance.

54. ***Securities Association of Singapore (SAS***): The SAS is the industry association for securities dealers in Singapore. SAS currently has 13 members, comprising largely the key securities brokers and SGX-ST members with a sizeable domestic clientele base.

55. ***Money Changers Association (MCA):*** The Singapore MCA comprises a group of money-changer licensees with about 40 to 50 members. Its objective is to provide a forum for discussion on money-changing issues.

56. ***Investment Management Association of Singapore (IMAS):*** The IMAS is a representative body of investment managers (companies). It aims to foster high standards of professionalism among practitioners, promotes the education of the investing public and represents the members' collective interest in discussions with MAS.

57. ***ACI Singapore (ACI):*** The ACI is affiliated to ACI – The Financial Markets Association, the global umbrella of national associations relating to the wholesale financial markets. ACI's objectives include keeping members informed of changes in the financial industry and providing a forum for discussion on issues affecting the markets and providing feedback to industry and authorities where needed. ACI's members are wholesale market practitioners (individuals) in trading, sales, management and operations of asset classes such as equities, commodities, currencies and interest rates.

58. ***Singapore Investment Banking Association (SIBA):*** The SIBA represents and furthers the interest of its member banks, including investment banks. SIBA serves as a forum for its members to discuss matters of common interest and a conduit between the industry and the relevant authorities.

(v) DNFBPs and other matters

59. ***Casino Regulatory Authority (CRA):*** The Casino Control Act (CCA) was passed in February 2006; however, it is not yet in force. Under its provisions, Ministry of Home Affairs will set up a statutory board, the CRA, to provide regulatory oversight and supervision of the casinos. Provisions of the CCA empower the CRA to investigate the casino operators' background, accounts and business links.

60. ***The Law Society*****:** The Law Society is a statutory entity responsible for regulating the Singapore legal profession.

61. ***Institute of Certified Public Accountants Society (ICPAS):*** The ICPAS is the national organization of the accountancy profession in Singapore with over 18 000 members, resident both in Singapore and overseas. ICPAS is a self-regulatory organization that sets auditing standards and issues guidance to its members, including the guidance on AML/CFT.

62. ***Singapore Jewellers Association:*** The Singapore Jewellers Association is a non-profit organisation that represents jewellery operators in Singapore. Currently, there are about 300 corporate members, including most of the reputable and long-established jewellers in Singapore. The Association's mission is to encourage members to follow a code of practice which is just and fair so as to protect the interests of the consumers and instil confidence in the trade among the general public.

63. ***Institute of Estate Agents (IEA):*** The IEA is a body that was formed by the merger of three real estate bodies in Singapore, namely the Association of Singapore Realtors (ASR), Association of Singapore Real Estate Agents (ASREA) and the Society of Singapore Institute of Surveyors and Valuers Accredited Estate Agents (SOCREA). The objectives of IEA are to promote and protect the interests of estate agents as well as to protect the interests of the general public engaging the services of estate agents.

64. ***Singapore Accredited Estate Agencies (SAEA) Scheme***: The SAEA Scheme, which was launched on 11 November 2005, is jointly administered by the Singapore Institute of Surveyors and Valuers (SISV) and the Institute of Estate Agents (IEA). SISV and IEA are the two major professional bodies representing estate agents in Singapore. The scheme sets the guidelines, minimum educational standards and practice standards for real estate agents.

65. ***Singapore Land Authority (SLA):*** The SLA is a statutory board under the Ministry of Law. Its mission is to optimize land resources for the economic and social development of Singapore. SLA has both developmental and regulatory roles. As a regulator, SLA is the national land registration authority and is also responsible for the management and maintenance of the national land survey system.

66. ***Accounting and Corporate Regulatory Authority (ACRA):*** ACRA is a statutory board established on 1 April 2004 under the Accounting and Corporate Regulatory Act. ACRA is the result of a merger between the former Registry of Companies and Businesses (RCB) and the Public Accountants Board (PAB). ACRA is the central registry for all business entities in Singapore including corporations, limited liability partnerships and sole proprietorships. ACRA is also the registry for the accounting profession.

c. Approach concerning risk

67. Singapore has adopted a risk-based approach in developing and implementing its AML/CFT regime.

68. ***Application of AML/CFT obligations to certain sectors:*** AML/CFT preventative measures apply to all financial institutions (as defined in the FATF Recommendations), with the minor exception of commodities futures brokers—a sector which the Singaporean authorities consider to be relatively low risk for ML/FT. Commodities futures brokers will be made subject to AML/CFT measures in 2008.[5]

69. ***Risk-based approach taken by financial institutions:*** MAS Notices and Guidelines provide some examples of low risk customers to whom financial institutions may apply simplified CDD measures. Financial institutions are required to apply enhanced CDD measures to customers determined to be high risk. This means that the financial institution must conduct a risk assessment to determine whether a customer is high or low risk.

70. ***Use of a Risk-Based Approach in Supervision:*** MAS uses an impact and risk model to allocate supervisory resources among institutions, and to distinguish those institutions that may pose a higher threat to the achievement of supervisory objectives. Undertaking business activities deemed to be susceptible to ML/FT risks has a bearing on the institutions' overall risk assessment, and hence such institutions are subject to more intensive supervision and more frequent on-site inspections (see section 3.10 of this report).

d. Progress since the last mutual evaluation or assessment

71. Singapore has systematically taken steps to address many of the recommendations that were made in its second FATF mutual evaluation in 1998-1999. The legislative and regulatory changes as well as institutional efforts to improve feedback to financial institutions, enhance supervisory oversight and step up training have resulted in a significant strengthening of Singapore's AML/CFT regime. The key recommendations identified for Singapore's systems are listed below, with a short summary of progress since then.

(a) ***Extend the money laundering offence to all indictable offences:*** The CDSA was amended to expand the money laundering offence and confiscation laws to a range of serious offences. The self-laundering and third party laundering offences were also expanded.

(b) ***Create an obligation for all persons to report suspicious transactions:*** The CDSA was amended to create a reporting obligation for all persons who, in the course of their trade, profession, business or employment, suspect that property relates to the proceeds of crime.

(c) ***Implement additional measures to improve the effectiveness of STR system:*** The CDSA was amended to address: (i) sanctions for failure to report suspicious transactions; (ii) full protection from criminal and civil liability if a report is made in a bona fide way; (iii) tipping-off offence; and (iv) government agencies giving feedback in relation to suspicious transaction reporting.

(d) ***Establish an FIU to deal with all aspects of an STR system:*** Singapore's FIU (STRO) became operational in January 2000.

(e) ***Issue legally binding AML/CFT Notices to different classes of financial institutions:*** MAS issued legally binding sector-specific AML/CFT notices that set out more clearly the legal obligations imposed on the financial institutions, and provide practical guidance on how these obligations are to be fulfilled.

(f) ***Increase feedback to financial institutions:*** STRO conducts extensive outreach and provides feedback to financial institutions.

---

[5] With effect from 27 February 2008, MAS assumed regulatory oversight of commodity futures: http://www.mas.gov.sg/legislation_guidelines/securities_futures/sub_legislation/Publication_of_MAS_Regulations_and_Notices_on_the_Transfer_of_Regulatory_Oversight_of_Commodity_Futures.html.

(g) ***Introduce a system to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments:*** Singapore has implemented a declaration system for this purpose.

(h) ***Implement additional measures on mutual legal assistance:*** Singapore enacted the MACMA to allow the Government to provide mutual legal assistance to other jurisdictions, in relation to criminal investigations or criminal proceedings for offences that are covered under the Act.

(i) ***Implement other measures to render assistance to foreign authorities:*** Amendments to the CDSA allow STRO to share information with foreign FIUs if there is an arrangement for such sharing on the basis of confidentiality and reciprocity.

(j) ***Remove the purposive element from the money laundering offence:*** The second FATF mutual evaluation report recommended that Singapore remove the purpose element of the predicate offence, which in addition to conceals, disguises, converts, transfers or removes property from the jurisdiction, also required that it be for the purpose of assisting another person to avoid prosecution for a serious offence or foreign serious offence, or the making or enforcement of a confiscation order. This purposive element remains for proving third-party money laundering, and this concern is discussed in greater detail in section 2 of this report.

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis

Recommendation 1

72. Singapore has criminalized ML in eight separate provisions of the CDSA. Three of these offences criminalise the laundering, acquisition and possession of proceeds generated by criminal conduct (ss.47(1) 47(2), and 47(3)). The others (which mirror the first three offences) criminalise the laundering, acquisition and possession of proceeds generated by drug trafficking (ss.46(1), 46(2), and 46(3)). Singapore also has two offences of assisting another to retain criminal proceeds: retaining or controlling another person's drug benefits (CDSA s.43) and retaining or controlling another person's benefits from criminal conduct (CDSA s.44). Singapore includes convictions under sections 43 and 44 in its statistics for ML convictions.

Consistency with the United Nations Conventions

73. Singapore's money laundering offences cover the conversion or transfer, concealment or disguise, possession and acquisition of property in a manner that is largely, but not wholly, consistent with the 1988 United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organised Crime (Palermo Convention). There is also a separate offence of laundering the proceeds of terrorist offences (s.6 TSOFA), which the Singaporean authorities characterise as a terrorist financing offence.

Concealing or transferring the benefits of criminal conduct: Section 47(1): self-laundering

74. Section 47(1) of the CDSA makes it an offence to launder the proceeds of criminal conduct through concealment, disguise, conversion, transfer or removal from the jurisdiction. Acquisition, possession, and use of the criminal property are now also explicitly covered per amendments to the CDSA effective 1 November 2007. The essential elements of the offence are.

(a) ***Physical element:*** The defendant conceals, disguises, converts, transfers or removes property from the jurisdiction, or acquires, possesses, or uses the property. The act of concealment or

disguise includes concealing or disguising the property's nature, source, location, disposition, movement or ownership or any rights with respect to it (s.47(4) CDSA).

(b) ***Mental/moral element:*** The defendant performed one of the actions enumerated above knowing or having reasonable grounds to believe that the property involved is, wholly or partly, the direct or indirect proceeds (benefits) of his benefits from criminal conduct.

(c) ***Predicate criminality:*** The proceeds (benefits) were generated from the commission of criminal conduct.

75. Where there is sufficient evidence to prove both the predicate offence and the laundering offence, a person can generally be charged for both distinct offences. Singapore has charged at least 14 cases involving both the predicate offence and an offence of self-laundering of the proceeds of that predicate offence.

Concealing or transferring the benefits of criminal conduct: Section 47(2): third-party laundering

76. Section 47(2) of the CDSA makes it an offence to launder the proceeds of criminal conduct through concealment, disguise, conversion, transfer or removal from the jurisdiction. The essential elements of the offence are:

(a) ***Physical element:*** The defendant conceals, disguises, converts, transfers or removes property from the jurisdiction. The act of concealment or disguise includes concealing or disguising the property's nature, source, location, disposition, movement or ownership or any rights with respect to it (s.47(4) CDSA).

(b) ***Mental/moral element:*** The defendant performed one of the actions enumerated above: (1) knowing or having reasonable grounds to believe that the property involved is, wholly or partly, the direct or indirect proceeds (benefits) of another person's criminal conduct; and (2) for the purpose of assisting another person to avoid prosecution for a serious offence or foreign serious offence, or the making or enforcement of a confiscation order.

(c) ***Predicate criminality:*** The proceeds (benefits) were generated from the commission of criminal conduct.

77. The Conventions require concealing or disguising to be an offence where the defendant knows that the property involved is the proceeds of crime (Palermo, Article 6(1)(a)(ii) and Vienna, Article 3(1)(b)(ii). The only mental element required by the Conventions is knowledge that the property is the proceeds of crime. However, section47(2) also requires proof that the property was concealed or disguised for the purpose of assisting another person to avoid prosecution for a serious offence, or the making of a confiscation order. The Conventions do not allow for any such purposive element in relation to concealing or disguising.

78. The Singaporean authorities indicate that, in practice, it would be possible to bring a prosecution under the 'possession' or 'use' limbs of section 47(3) based on the same set of facts, because a person who conceals or disguises property would logically have had possession of or have used such property. However, to date, no prosecutions have been brought under section 47(3). In any event, the Singaporean authorities are considering steps to de-link this particular type of third-party laundering offence from the requirement to prove a purpose.

79. A further technical problem arises in relation to the conversion or transfer of property. The Conventions require the conversion or transfer of property to be an offence where the defendant knows that the property involved is the proceeds of crime and does so for one of the following two purposes: (1) concealing or disguising its illicit origin; *or* (2) for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action (Palermo, Article 6(1)(a)(i) and Vienna, Article 3(1)(b)(i). However, section 47(2) sets out only one purpose element (for the purpose of assisting another person to avoid prosecution for a serious

offence or foreign serious offence, or the making or enforcement of a confiscation order) instead of the two alternatives permitted by the Convention.

80. The Singaporean authorities report that these technical problems relating to *mens rea* and purpose have so far not impeded their ability to prosecute this ML offence. To date six cases have been brought pursuant to third party money laundering, including two cases under section 47(2). Four cases involved prosecutions under sections 43 and 44 for arranging with third parties to retain their own criminal benefits, which are not offences specifically covered by the Conventions. Of these six cases, five (including both s.47(2) cases) resulted in convictions and one case is pending trial.

81. It should also be noted that the self-laundering offence described above, section 47(1), does not suffer from either of these two deficiencies in relation to *mens rea*.

Concealing or transferring the benefits of drug trafficking: Sections 46(1) and (2)

82. Sections 47(1) and (2) of the CDSA (described above) are virtually identical to sections 46(1) and (2), except for the fact that they apply to the proceeds (benefits) generated from the commission of drug trafficking. Section 46(2), the third party money laundering offence relating to drug trafficking proceeds, suffers from the same deficiencies that are described above in relation to section 47(2). In other words, in relation to concealment and disguise, the prosecution must prove additional elements of mens rea that are not in line with the Conventions and, in relation to conversion or transfer, the offence sets out only one purpose element instead of the two alternatives required by the Convention. Like section 47(1), the self-laundering offence, section 46(1), does not suffer from these deficiencies. The views of the Singaporean authorities expressed above in relation to sections 47(2) apply equally to section 46(2).

Acquiring, possessing, and using the benefits of criminal conduct: Sections 47(1) and 47(3)

83. Recent amendments to section 47(1) of the CDSA extend the criminalisation of self-laundering to the acquisition, possession or use of such property (see above description). Section 47(3) (which originally only criminalised the knowing acquisition of proceeds generated by another person's criminal conduct for no or inadequate consideration) was similarly extended to include possession or use. The essential elements of section 47(3) are:

(a) ***Physical element:*** The defendant acquires property for no or inadequate consideration, or has possession of or uses the property.

(b) ***Mental/moral element:*** The defendant knows or has reasonable grounds to believe that the property is, wholly or partly, the direct or indirect proceeds (benefits) of another person's criminal conduct.

(c) ***Predicate criminality:*** The other person's proceeds (benefits) were generated from the commission of criminal conduct.

84. Section 47(3) requires an additional element of proof that is inconsistent with the Conventions – that the defendant acquired the property for "no or inadequate consideration". The Conventions require the criminalization of the mere acquisition, possession or use of property knowing that, at the time of receipt, the property was derived from a predicate offence. The Singaporean authorities indicate that this additional element of proof is intended to protect tradesmen who have paid fair value for the property that they are in possession of. However, this approach creates a gap in Singapore's ability to prosecute someone who pays fair value for property, knowing that this property is the proceeds of crime. Nevertheless, the impact that this gap has on Singapore's ability to prosecute such persons is mitigated by the fact that a third person who has "acquired" property (regardless of the value of any consideration paid) presumably would have been in possession of that property. The recent amendments would appear to permit Singapore to prosecute such a person for possession of proceeds – an offence that does not require the additional element of proof regarding lack of or inadequate consideration required by the acquisition offence.

Acquiring, possessing, and using the benefits of drug trafficking: Sections 46(1) and 46(3)

85. Section 46(3) of the CDSA is virtually identical to section 47(3) described above, except for the fact that it applies to another person's proceeds (benefits) generated from the commission of drug trafficking. It suffers from the same minor technical deficiency in that an additional element of proof, inconsistent with the Conventions, is required.

Assisting another person to retain the benefits of criminal conduct: Section 44(1)

86. Section 44(1) of the CDSA makes it an offence to enter into an agreement to facilitate the retention or control, by or on behalf of another person, of that person's criminal proceeds or benefits (*e.g.* by concealment, removal from the jurisdiction, transfer to nominees, acquisition, use or otherwise). The essential elements of the offence are:

(a) ***Physical element:*** The defendant entered into or was otherwise concerned in an arrangement that:

  (i) Facilitates another person's retention or control of that other person's benefits of criminal conduct (*e.g.* by concealment, removal from the jurisdiction, transfer to nominees or otherwise). Or

  (ii) Uses another person's benefits of criminal conduct to secure funds that are directly or indirectly placed at that other person's disposal, or are used for that other person's benefit to acquire property by way of investment or otherwise.

(b) ***Mental/moral element:*** The defendant enters into or is otherwise concerned in an arrangement, knowing or having reasonable grounds to believe that: (1) the purpose of the arrangement is one of those listed above; and (2) the other person carries on (or has carried on) criminal conduct or has benefited from criminal conduct.

(c) ***Predicate criminality:*** The other person's proceeds (benefits) were generated from criminal conduct.

Assisting another person to retain the benefits of drug trafficking: Section 43(1)

87. Section 43(1) of the CDSA is virtually identical to section 44(1), except for the fact that it applies to another person's proceeds (benefits) generated from the commission of a drug trafficking offence.

Laundering the proceeds of terrorist offences: Section 6 TSOFA

88. Singapore has also specifically criminalised the laundering of the proceeds of terrorist offences pursuant to section 6 of the TSOFA. Section 6 criminalises three types of activity and applies to any person in Singapore or any Singaporean citizen outside of the country. It targets the laundering of property of individual terrorists of terrorist organisations as follows: (a) dealing in property with the knowledge (or reasonable grounds to believe) that the property is owned or controlled by or on behalf of any terrorist or terrorist entity; (b) entering into or facilitating any financial transaction related to a dealing in such property; and (c) providing any financial services or any other related services in respect of such property for the benefit of, or on the direction or order of, any terrorist or terrorist entity. The term "terrorist entity" is defined to mean any entity owned or controlled by any terrorist or group of terrorists and includes an association of such entities. "Entity" in turn means a person, group, trust, partnership or fund or an unincorporated association or organization (s.2(1) TSOFA).

Definition of proceeds

89. All of Singapore's money laundering offences extend to "property" which is defined in the CDSA to include money and all other property, moveable or immovable, including things in action and other intangible or incorporeal property, and wherever situated that, in whole or in part, directly or

indirectly, represents the benefits of drug trafficking or criminal conduct (ss.2(1) and 3(5)). There is no value threshold. Both the direct and indirect proceeds of crime are covered (ss.43(2), 44(2), 46(3) and 47(3) CDSA). A similarly broad definition of "property" is contained in section 2(1) of the TSOFA and applies to the specific offence of laundering the proceeds of terrorist offences.

90. The CDSA provisions criminalizing money laundering do not require a conviction of an underlying alleged predicate offence in order to prove offences under sections 43, 44, 46, or 47. Although this issue is not specifically addressed in the CDSA, this position is confirmed by recent case law in which two ML convictions were obtained in the absence of convictions for the predicate offences.

Predicate offences

91. Singapore has adopted a list approach to define the scope of predicate offences. As at 14 November 2007, there were 335 predicate offences for money laundering. Predicate offences for laundering the proceeds generated by drug trafficking pursuant to sections 46(2), 46(3) and 43(1) are listed in the First Schedule of the CDSA, and include trafficking, manufacturing, importing, exporting and cultivating controlled drugs. Predicate offences for laundering the proceeds generated by criminal conduct pursuant to sections 47(2), 47(3) and 44(1) are defined as being the 329 serious offences that are listed in the Second Schedule of the CDSA (s.2(1) CDSA).[6]

92. The predicate offences set out in the First and Second Schedule of the CDSA include a range of offences in each of the 20 categories designated by the FATF.

93. Singapore has not enacted a separate offence of "human trafficking"; however, its laws provide a piecemeal approach which largely covers the acts contemplated by the UN Conventions and Protocols. Singapore's offences are limited to: (1) trafficking in women and girls, for the purpose of prostitution (ss. 141 and 142 of the Women's Charter); (2) importing, exporting and dealing in slaves (Penal Code (PC), ss. 370-371); (3) hiring and disposing of persons under 21 for prostitution purposes (PC, ss. 372-373); and (4) the importation into Singapore any woman for prostitution purposes (PC, s. 373A). A broad range of migrant smuggling offences is also criminalised.[7] These offence cover smuggling, or otherwise conveying, prohibited immigrants into Singapore. This range of offences is sufficiently broad to meet the requirements of Recommendation 1.

94. In relation to the designated category of "participation in an organised criminal group and racketeering", Singapore has not separately criminalised participation in an organised criminal group or racketeering. However, the Penal Code contains broad conspiracy provisions (described below) that apply to all criminal offences in Singapore, and would therefore presumably apply to the range of profit-generating predicate offences committed by organised criminal groups and meet the requirements of Recommendation 1. However, Singapore has not prosecuted ML based on the predicate offence of conspiracy to commit racketeering type offences.

95. Conduct that occurs in another jurisdiction may constitute a predicate offence for ML if such conduct, had it occurred in Singapore, would constitute a predicate offence, provided that the dual criminality requirement is met. The concept of "criminal conduct" in ML offences under Sections 44 and 47, CDSA includes "foreign serious offences" which are defined as offences against the laws of a foreign country where the act or omission constituting the offence or the equivalent act or omission would have constituted a serious offence had it occurred in Singapore. This same principle applies to a predicate drug trafficking offence for the purpose of establishing a ML offence in Singapore under sections 43 and 46 CDSA. The offence of laundering terrorist property under section 6 of the TSOFA applies to all persons in Singapore and Singapore citizens outside of Singapore. A Singapore citizen

[6] Amendments to the CDSA, effective 1 November 2007, added 36 offences to the First and Second Schedules.

[7] Immigration Act (Cap. 133); see also the case of Pub. Prosecutor v. Tay Boon Hua @ Ah Chai (11 June 2004).

who commits this offence in any place outside of Singapore may be prosecuted as if the offence had occurred in Singapore (s.34(2) TSOFA).

96. There is a broad range of ancillary offences to the money laundering offences, which are set out in sections 109 to 117 of the Penal Code. These general provisions apply to all criminal offences. These "abetment" offences are defined in section 107 of the Penal Code to include conspiracy (by two or more persons to commit an offence), aiding an offence by any act or illegal omission, or instigating an offence.[8] Explanations in the Penal Code also make it clear that the concept of "aiding" includes facilitating. Case law confirms that the "instigation" provision of the abetment provisions also cover the factual scenario of one person counselling another to commit a criminal offence.[9] Attempt is criminalized by section 511 of the Penal Code.

Additional elements

97. The CDSA defines "criminal conduct" as doing or being concerned in any act constituting a serious offence (*i.e.* a predicate offence) whether in Singapore or elsewhere. Hence, even if the country where the conduct occurred does not criminalize the conduct, so long as the conduct constitutes a predicate offence had it occurred in Singapore, deriving proceeds of crime from such conduct can still constitute a ML offence in Singapore pursuant to sections 44 or 47 of the CDSA.

Recommendation 2

Scope of liability

98. The ML offences apply to all "persons". Section 2(1) of Interpretation Act (the provisions of which apply to all written laws) defines "person" as including any company or association or body of persons, corporate or unincorporated. This includes a "society" pursuant to section 2(1) of the Societies Act (*e.g.* a club, company, partnership or association of 10 or more persons, whatever its nature or object) or an unincorporated person such as a sole proprietorships or partnership of a "business" (defined in section 2(1), Business Registration Act (BRA) to include every form of trade, commerce, craftsmanship, calling, profession and any activity carried on for the purposes of gain).

99. In the case of legal persons, criminal liability for ML may be established by proof that a director, employee, or agent commits, or directs, consents, or agrees to the ML act within the scope of his/her actual or apparent authority (s.52 CDSA). Where a legal person or a body corporate is found guilty of a CDSA ML offence that is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of any of its key officer, both the officer and the body corporate shall be guilty of that offence (s.59 CDSA). Legal persons subject to criminal liability for ML can face parallel criminal, civil and administrative proceedings and actions in Singapore. Singapore has not yet prosecuted a corporate or unincorporated body pursuant to the CDSA.

100. It is well established by Singapore case law that the requisite intentional element of the offence of money laundering may be inferred from objective factual circumstances. [10]

---

[8] Section 2(1) of the Interpretation Act provides that "abet", with its grammatical variations and cognate expressions, has the same meaning as in the Penal Code, and this interpretation applies to every written law.

[9] *Public Prosecutor v Ng Ai Tiong* [2000] 1 SLR 454.

[10] Loh Kim Cheng v Public Prosecutor [1998] 2 SLR 315; Mohd Zin bin Atan & Anor v Public Prosecutor [1999] SGCA 56 (Court of Appeal).

Sanctions

Criminal sanctions

101. For ML offences under sections 43 and 44 of the CDSA, natural persons are liable to a maximum fine of SGD 200 000 and/or imprisonment of up to 7 years, while legal persons are liable to a maximum fine of SGD 200 000. Amendments effective November 2007, increased the fines for sections 46 and 47 of the CDSA to SGD 500 000 for natural persons and SGD 1 000 000 for legal persons. The TSOFA offence of laundering the proceeds of terrorist offences is punishable by a maximum fine of SGD 100 000 and/or imprisonment of up to 10 years in the case of natural persons, and a maximum fine of SGD 100 000 in the case of legal persons. In terms of proportionality, these prescribed maximum penalties are on par with most of the other serious economic crimes in Singapore (*e.g.* cheating, dishonesty, forgery and falsification of accounts) and are also proportionate to the penalties for ML in other countries in the region (*e.g.* Indonesia – 5 to 15 years; Malaysia – 7 years; Philippines – 7 to 14 years; Australia – 5 to 25 years).

Civil liability

102. If a legal person commits an ML offence and in the process causes harm to another person, the legal person can incur both criminal and civil liability (s.39 Interpretation Act).

Administrative proceedings/measures

103. Upon conviction for money laundering pursuant to the CDSA, a company may be wound up, a foreign company may be de-registered, the registration of business of a sole proprietorship may be cancelled, and a society may be dissolved (s.24 CDSA). Such administrative liability is imposed in addition to criminal liability, which takes the form of a fine for legal persons.

104. Even without a conviction, the High Court may order the winding up of a company that is being used for an unlawful purpose or for purposes prejudicial to public peace, welfare or good order in Singapore (s.230, et seq., Companies Act) or against national security or interest (s.254(1)(m), Companies Act). The Minister charged with the responsibility for internal security must state that he is satisfied that the company referred to in the certificate is being used for such purposes, and where the Registrar of Companies is satisfied, he/she shall cancel its registration. Similar provisions apply to foreign companies registered in Singapore (s.377(8), Companies Act) and unincorporated societies. (Societies Act).

105. If convicted of ML in circumstances arising from a corruption offence involving bribery of public servants or other persons in connection with a government agency or contract, a legal person may also be debarred from tendering for government projects for a minimum of 5 years, regardless of the amount involved, and shall have their tender deposits (if any) forfeited (paragraph 189, Government Instruction Manuals (IM3G: Revenue Contracting Procedures, Penalties and Debarment). The directors, partners or sole proprietors of the debarred companies or businesses who are involved in corruption or rigging, other companies or businesses on which the blacklisted directors or partners or sole proprietors sit, and the existing and new subsidiaries of the principal offending company can also be debarred (paragraph 782, Government Instruction Manuals (IM3B: Contracts and Purchasing Procedures, Debarment of Contractors)). The relevant government registration authority would also inform the principal offending companies or businesses and blacklisted directors or partners or sole proprietors (through the debarred companies or businesses) of the sanctions against them. Such sanctions would include sanctions by the ministries, departments, statutory boards and certain government-linked companies, against their subsidiaries and other companies/businesses on which the blacklisted directors/partners/sole proprietors sit.

Recommendation 32 (Money laundering investigation/prosecution data)

Statistics and effectiveness

106. The key agencies involved in ML and TF investigations maintain their own set of statistics in accordance with their operational requirements. These statistics include the number of ML and TF investigations, prosecutions and convictions, including investigations arising from STRs and as a result of predicate offences. These statistics are then reported to the heads of the respective agencies that put them up for consideration and review by the IAC, respectively.

107. Between 1 January 2007 and 14 November 2007, Singapore has obtained a total of six convictions under the CDSA. This includes 5 money laundering convictions as well as one conviction for failure to disclose under section 39 CDSA. Singapore has therefore obtained 25 ML convictions between 2000 and 14 November 2007.[11] Although it is recognised that Singapore has a very low domestic crime rate, this number seems low given the high incidence of drug trafficking and corruption offences in other countries of the region, and Singapore's attractiveness as a stable financial centre through which criminals might launder the proceeds of predicate offences committed abroad. It also appears from the statistics provided in the chart below, that the number of prosecutions and convictions obtained each year has declined since the early 2000's, when the CDSA was first being utilized. There is an improvement in 2007; however, it is not yet clear if this is an exception or a trend.

108. Moreover, nearly all of the ML cases charged are for self laundering (s.47(1) or other offences under the CDSA. Third-party laundering cases (*e.g.* s.43(1)(a) and s.47(2)) have only recently been pursued, and two convictions were obtained during 2007 (up to 14 November). This raises the question of whether the additional purposive element of s. 47(1) (to assist another to avoid prosecution or confiscation) is hindering prosecutions being brought forward for these cases.

Convictions under the CDSA (2000-14 November 2007)[12]

Year	Number of Convictions	Section of CDSA Charges (Cap 65A) Proceeded	Punishment TIC = Taken into consideration	Sum of Money Laundered (Based on Charges Tendered)	Total Length of Sentences
2000	4	(1). s.43A(1)(a) [13]	TIC (concurrent of 2 years imprisonment for other charges)	USD 9 250 000	24 years
		(2). s.43A(1)(a)	24 months imprisonment (consecutive)	USD 260 000	6 years
		(3). s.43A(1)(a) s. 43A(1)	24 months imprisonment (concurrent) TIC	USD 260 000	6 years

[11] The total number of convictions in 2007 under the CDSA has increased to 13 as at 31 December 2007 and this includes 12 money laundering convictions and one conviction for failure to disclose under section 39 CDSA. As such, the total number of ML convictions has increased to 32 as at 31 December 2007.

[12] Between 15 November and 31 December 2007, an additional 9 ML charges proceeded, including 2 more charges for third party ML pursuant to s.47(2)(a). The breakdown of ML offences charges during this period is: 2 ML charges under s.44(1)(a);3 ML charges under s.47(1)(a); 2 ML charges under s.47(1)(b); and 2 ML charges under s.47(2)(a). In total, from 2000 to 31 December 2007, a total of 52 ML charges proceeded and 33 convictions were obtained.

[13] This reference to s.43A(1)(a) CDSA (Cap 85A), is the equivalent of section 47(1)(a) of the present CDSA (Cap 65A), as referred to in this report.

Year	Number of Convictions	Section of CDSA Charges (Cap 65A) Proceeded	Punishment TIC = Taken into consideration	Sum of Money Laundered (Based on Charges Tendered)	Total Length of Sentences
		(4). s.43A(1)(b) s.43A(1)(b)	48 months imprisonment (consecutive) TIC	AUD 980 000	8 years
2001	1	(1) s.47(1)(b)	18 months imprisonment (concurrent)	USD 50 000	6 years
2002	6	(1). s.47(1)(b)	36 months imprisonment (concurrent)	USD 592 000	22 years
		(2). s.47(1)(b) s47(1)*	24 months imprisonment (consecutive) 24 months imprisonment(concurrent)	USD 438 000	87 months
		(3). s.43A(1) s.47(1)(a) s.47(1)(b) s.47(1)(b)	24 months imprisonment (concurrent) 24 months imprisonment (concurrent) 24 months imprisonment (consecutive) 24 months imprisonment (concurrent)	USD 2 200 000	8 years
		(4). s.47(1)(b)	24 months imprisonment (consecutive)	USD 143 000	12 years
		(5). s.47(1)(b) s.47(1)(b)*	24 months imprisonment TIC	USD 79 500	2 years
		(6). s.47(1)(b)	24 months imprisonment (consecutive)	USD 183 000	78 months
2003	3	(1). S.47(1)(b)	24 months imprisonment (consecutive)	USD 462 500	4 years
		(2). s.47(1)(a) s.47(1)(a)	20 months imprisonment (consecutive) TIC	USD 242 000	52 months
		(3). s.47(1)(b)	24 months imprisonment (consecutive)	SGD 565 000	30 months
2004	2	(1). S.47(1)(a) (2 counts)	TIC	SGD 1 500 000 AUD 8 800 000	42 years
		(2). s.47(1)(b) s.47(1)(b)	10 months imprisonment +SGD 20 000 fine (consecutive) 2 months imprisonment +SGD 20 000 fine (consecutive)	SGD 26 000	12 months & SGD 40 000 fine
		s.47(1)(b)	TIC		

Year	Number of Convictions	Section of CDSA Charges (Cap 65A) Proceeded	Punishment TIC = Taken into consideration	Sum of Money Laundered (Based on Charges Tendered)	Total Length of Sentences
		s. 47(1)(b)	TIC		
2005	2	(1). S.47(1)(b)	6 months imprisonment (concurrent)	USD 400 000	5 years
		(2). s.43(1)(a) s.43(1)(a)	14 months imprisonment TIC	SGD 33 000	14 months
2006	2	(1). s.47(1)(b) s.47(1)(b) s.47(1)(b)	36 months imprisonment (consecutive) 24 months imprisonment (concurrent) 24 months imprisonment (concurrent)	SGD 4 200 000	8 years
		(2). s.47(1)(b) s.47(1)(b)	2 months imprisonment (consecutive) 2 months imprisonment (concurrent)	SGD 70 000	18 months & SGD 20 000 fine
2007 (to 14 Nov.)	6	(1). s.47(1)(b)	TIC	SGD 850 000	90 months
		(2). s.47(1)(a)	2 months (concurrent)	MYR 50 000	2 months
		(3). s.39 (1)	SGD 5 000 fine and in default 5 weeks imprisonment	GBP 1 600	SGD 5 000
		(4). s.47(2)(a) (2 counts)	4 months imprisonment (concurrent)	SGD 5 700	4 months
		(5). S47(1)(a) S.47(1)(a)	4 months and SGD10 000 fine TIC	SGD 22 400	4 months & SGD 10 000 fine
		(6). S47(1)(b)	15 months imprisonment	SGD 8 3584.27	15 months
TOTAL NUMBER OF CDSA CONVICTIONS 26			**43 ML Charges Proceeded**		

*Read with s.109 Penal Code (Abetting offence).

109. From the above chart, it appears that the penalties being applied are not very dissuasive. Of the 43 charges of money laundering for which convictions were obtained, over half were either sentenced to less than 18 months imprisonment or taken into consideration for the purposes of sentencing. In the three instances where fines were imposed, the highest was only SGD 20 000 (approximately EUR 9 300). The low level of sanctions actually being imposed in practice, suggests that the penalties for money laundering are not being applied effectively.

110. The overall level of money laundering convictions also seems extremely low, particularly given the size of Singapore's financial sector (which is about one tenth the size of Switzerland's measured in terms of private assets under management) and its acknowledged level of ML risk. Overall, the statistics suggest that Singapore is overly focused on prosecuting predicate offences (primarily based on domestic crime). Singapore has, generally, not aggressively pursued money laundering as a separate crime in the past. This is particularly so in relation to third party laundering,

through Singapore's financial system, of proceeds generated by foreign predicate offences. Singapore is encouraged to continue the focus it has shown in several international money laundering cases, and to prioritize these cases, in addition to the stated priorities of illegal money lending and laundering of gambling proceeds.

111. Singapore authorities have also argued that its low statistics are due to the country's low domestic crime rate which results in few predicate offences that generate significant proceeds of crime. However, this does not account for the low number of convictions (two as of 14 November 2007) in which predicate offences may have been committed abroad (such as official corruption) and Singapore, as a major financial centre, is used to launder the funds domestically, such that funds may be invested in financial institutions in Singapore (for a further discussion of these issues see sections 2.3, 2.5 and 2.6 of this report). These statistics clearly highlight that the authorities are focused on pursuing predicate offences, with money laundering as an ancillary offense. Nevertheless, it should also be noted that, despite the low domestic crime rate, there are still clearly crimes occurring in Singapore that create opportunities for prosecuting, not just self-laundering, but also third-party ML cases (see the statistics of convictions relating to predicate offences set out in section 1.2 of this report).

112. In most cases, the law enforcement authorities appear to build their ML cases to the point where they can clearly identify and prove the predicate offence (generally a domestic one) that generated the proceeds, before referring them to the AGC for prosecution. For example, of the 38 ML referrals and complaints it received from 2004 to 2006, the CAD, as at the time of the onsite was investigating 9 cases with a view to identifying the predicate offence that generated the proceeds. On 15 out of the 23 completed cases, the CAD determined that insufficient evidence existed to charge ML, although 11 of these cases resulted in conviction for a predicate offence.

113. That the authorities generally prosecute ML cases when they are also able to prosecute the underlying domestic predicate offence, as opposed to ML as a separate crime (perhaps based on foreign predicates), is demonstrated by the disproportionately low number of ML cases being referred to the AGC for prosecution by the CAD in relation to the large number of STRs being filed (3 290 in 2006) – although when ML prosecutions are referred to the AGC, the conviction rate is very high (almost 100%), and inevitably result in jail sentences. Between 2004 and 14 November 2007, the CAD referred only 36 ML cases to the AGC for prosecution, the outcomes of which are set out in the chart below.

Outcome of CDSA Cases Referred for Prosecution by CAD between 2004 and 14 Nov 2007

Outcome	2004	2005	2006	2007 (to 14 Nov)	Total
Under Legal Assessment	0	1	3	4[14]	**8**
AGC directed to take NFA	1	1	2	0	**4**
Prosecuted and Pending trial/decision	0	0	3	10[15]	**13**
Convicted	2	1	2	6[16]	**11**
Total	**3**	**3**	**10**	**20**	**36**

[14] 25 as of 31 December 2007.

[15] 5 as of 31 December 2007.

[16] 13 as of 31 December 2007.

Additional elements

114. The authorities maintain comprehensive statistics concerning the criminal sanctions that are applied to persons convicted of money laundering (see the above chart for details).

2.1.2 Recommendations and Comments

115. The main issue is that Singapore's money laundering offences are not being effectively implemented. Although much of the criminal activity may be caught "at the door" with proactive financial sector education, and compliance inspections (see section 3 of this report for further details), there seems to be less emphasis and priority placed on obtaining convictions for ML than for obtaining convictions on other criminal activity (*i.e.* predicate offences). The fact that a large number of STRs have been filed each year is indicative of suspected movement and attempted movement of criminally-derived property through Singapore's financial system. However, Singapore appears to be hesitant to aggressively pursue domestic prosecutions for ML cases involving foreign predicates. The assessment team was not able to fully determine the reasons for this hesitancy. Several explanations were provided, including that sentences for predicate offences were sufficiently high to deter future activity, and it was not, therefore, necessary to also prosecute for ML. However, this explanation does not address instances where the proceeds of foreign predicate offences are being laundered through Singapore. It also does not explain why the number of money laundering convictions was generally higher in 2000, 2001, and 2002, than in later years. There is an improvement in 2007; however, it is not yet clear if this is an exception or a trend.

116. Singapore should more aggressively pursue ML as a stand-alone offence, with a view to deterring ML by both its own citizens and foreigners who are using the Singapore financial sector (from foreign PEPs to foreign migrant workers using the local hawala systems). Finally, Singapore should remove the additional purpose elements in its third-party money laundering offences of concealment or disguise, and add the additional alternative purpose element to its third-party money laundering offences of convert or transfer, which might also allow more prosecutions for this kind of activity to be brought forward.

117. There have been no prosecutions of legal persons for ML offences, although it is also not clear that any such cases have arisen. As well, Singapore should ensure that sanctions are more effectively applied to persons convicted of money laundering.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	**PC**	• Effectiveness: The money laundering offence is not effectively implemented as is shown by: the low number of ML prosecutions and convictions, given the size of Singapore's financial sector and the level of ML risk. Also there is a focus on pursuing domestic predicate offence cases, with ML as an ancillary crime, rather than ML as a separate offence, which results in few third party ML cases being pursued and insufficient attention being paid to ML involving the proceeds of foreign predicate offences. • An additional "purposive" mens rea requirement in CDSA Sec. 46(2) and 47(2) in relation to the offence of "concealment or disguise", and a missing alternative purpose element in relation to the offence of "conversion or transfer" are inconsistent with the Conventions and may hamper the government's ability to prosecute third-party ML cases under those sections.
R.2	**LC**	• The money laundering offence is not effectively implemented as is shown by the low number of overall ML prosecutions and convictions (given the size of Singapore's financial sector and the level of ML risk), the low range of sentences being applied, and the focus on pursuing domestic predicate offences rather than ML which results in few third-party ML cases being pursued and insufficient attention being paid to ML involving the proceeds of foreign predicate offences. No prosecutions have been brought against any legal persons.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Characteristics of the terrorist financing offence

118. Singapore has criminalised four main terrorist financing offences (sections 3-5, Terrorism (Suppression of Financing) Act (TSOFA)).

Provision or collection of property for terrorist acts (section 3 TSOFA)

119. Section 3 of the TSOFA prohibits the provision or collection of property by any person for terrorist acts. The essential elements of the offence are:

(a) ***Physical element:*** The defendant directly or indirectly, wilfully and without lawful excuse, provides or collects property.

(b) ***Mental/moral element:*** Intending or knowing, or having reasonable grounds to believe, that such property will be used, in whole or in part, in order to commit any terrorist act.)

120. The UN International Convention for the Suppression of the Financing of Terrorism (FT Convention) requires countries to criminalise the financing of two types of acts: (1) the financing of the acts set out in the Conventions and Protocols referred to in the FT Convention's Annex (article 2(1)(a) and (2) "Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act"(article 2(1)(b).

121. In relation to the second of these elements, the definition of "terrorist act" in section 2(2) of the TSOFA largely comports with the definition in article 2(1)(b) of the FT Convention. The TSOFA definition includes the use or threat of action which is intended (or reasonably regarded as intending) to: (1) intimidate the public; or (2) influence or compel a government or international organisation from doing (or refraining from doing) any act. Such action, includes any action specified in the schedule to the TSOFA, and must also:

(a) Involve serious violence against a person, endanger a person's life, or create a serious risk to the health or safety of the public.

(b) Involve serious damage to property.

(c) Involve the use of firearms or explosives.

(d) Involve the release into the environment or a distribution exposing the public to any dangerous, hazardous, radioactive or harmful substance, toxic chemical, toxin, or microbial or biological agent.

(e) Disrupt, or seriously interfere with, any public computer system or the provision of any service directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure.

(f) Disrupt, or seriously interfere with, the provision of essential emergency services (*e.g.* police, civil defence and medical services). Or

(g) Prejudice the public security or national defence.

122. The schedule to the TSOFA includes offences that are listed under Singapore's Hijacking of Aircraft and Protection of Aircraft and International Airports Act (Cap. 124), but does not include all offences listed in the conventions and protocols shown in the Annex to the FT Convention, as required by article 2(1)(a).While many of the acts contemplated in the Conventions and Protocols in the Annex

to the Convention might be criminal acts in Singapore, they would only be considered terrorist acts if they were also committed with the intent to intimidate the public or influence or compel a government to action/inaction, etc. These required purposive elements go beyond the requirements of article 2(1)(a) of the FT Convention, which require that the acts be considered terrorist acts without the need to prove any additional intent. Therefore, financing of these acts would not be considered terrorist financing in Singapore. Singapore has indicated that it intends to expand the list of terrorist acts in the TSOFA schedule as and when it accedes to the various terrorist Conventions and Protocols referred to in the FT Conventions Annex.

Provision of property and services for terrorist purposes (section 4 TSOFA)

123. Section 4 of the TSOFA prohibits the provision or solicitation by any person of property and/or services for terrorist purposes. The essential elements of the offence are:

(a) ***Physical element:*** The defendant, directly or indirectly, collects property, provides or invites a person to provide, or makes available property or financial or other related services.

(b) ***Mental/moral element:*** Intending, or knowing, or having reasonable grounds to believe, that the property or services will be used to facilitate or carry out any terrorist act, to benefit any person who is facilitating or carrying out a terrorist act, or will be used by or benefit any terrorist or terrorist entity.

Prohibiting the use and possession of property for terrorist purposes (section 5 TSOFA)

124. Section 5 of the TSOFA goes beyond the requirements of Special Recommendation II in that it creates terrorist financing offences of use and possession. Section 5(a) of the TSOFA prohibits the use by any person of property for terrorist purposes. The essential elements of the offence are:

(a) ***Physical element:*** The defendant uses property, directly or indirectly, in whole or in part.

(b) ***Mental/moral element:*** for the purpose of facilitating or carrying out any terrorist act.

125. Section 5(b) of the TSOFA prohibits the possession by any person of property for terrorist purposes. The essential elements of the offence are:

(a) ***Physical element:*** The defendant possesses property.

(b) ***Mental/moral element:*** intending, or knowing, or having reasonable ground to believe, that the property will be used to facilitate or carry out a terrorist act.

Other terrorist financing offences contained in subsidiary legislation

126. There are also a number of offences under subsidiary legislation that are broadly similar to the terrorist offences set out in sections 3, 4 and 6 of the TSOFA, and which are primarily aimed at persons designated pursuant to the UN Consolidated List of terrorist and terrorist organizations. The UN (Anti-terrorism Measures) Regulations (UN (ATM) Regs) contain FT offences prohibiting anyone, except a financial institution covered under MAS (dealt with under the Regulations below-noted) from providing or collecting funds for terrorists, dealing with property of terrorists, and provision of resources and services for benefit of terrorists (UN (ATM) Regs R.5-7). Likewise, the Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations (2002) (S515/2002) (MAS (ATM) Regs) contain offences prohibiting financial institutions from providing or collecting funds for terrorists, dealing with property of terrorists, provision of resources and services for benefit of terrorists, and doing anything that causes, assists or promotes an act contrary to the aforesaid prohibitions (MAS (ATM) Regs R.5 -8).

Definition of "property"

127. The definition of "property" in the TSOFA is identical to the definition of "funds" in Article 1 of FT Convention. The broad definition of property in the TSOFA would include both legitimate and illegitimate assets. It is clear from the definition of "terrorist act" (which includes the threat to carry out a terrorist act) that the terrorist financing offences do not require that the funds were actually used to carry out or attempt a terrorist act, or that they are linked to a specific terrorist act.

Ancillary offences

128. The TSOFA sets out a full range of ancillary offences to all four of the terrorist financing offences described above, including conspiracy to commit, inciting another to commit, attempting to commit, aiding, abetting, counselling or procuring the commission of the offence: section 2(1) (also see section 107-120, Penal Code). In addition, an attempt to commit any of the offences provided for in TSOFA is criminalised in section 511 of the Penal Code.

Predicate offences for ML and jurisdictional issues

129. The terrorist financing offences in sections 3 to 5 of the TSOFA and the offence of laundering the proceeds of terrorist offences in section 6 of the TSOFA are predicate offences for ML, as are the FT offences set out in the UN (ATM) Regulations R.5-7 and the MAS (ATM) Regulations R.5-8 (see para. 278-281, 286 and 248 of Second Schedule of the CDSA respectively).

130. Singapore's FT offences apply regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist or terrorist organization is located or the terrorist act occurred or will occur. References to person or property for the purposes of "terrorist act" cover any person or property wherever situated, within or outside Singapore, and "public" includes the public of a country or territory other than Singapore (s.2(4) TSOFA). Therefore, while a terrorist act may be committed against a person or property or the public outside Singapore, if the FT offence is committed in Singapore, the perpetrator can be prosecuted in Singapore under sections 3 to 6 of the TSOFA. These FT offences can also be applied, regardless of where the "terrorist" and "terrorist entity" (defined generally in s.2(1), TSOFA) might be situated.

131. Additionally, the TSOFA has adopted universal jurisdiction for FT offences. If any person outside of Singapore commits an act or omission which would constitute an FT offence under sections 3, 4 or 5 of TSOFA (or an abetment, conspiracy or attempt to commit such offence if committed in Singapore), he/she can be prosecuted in Singapore, regardless of the location of the terrorist, terrorist organization and terrorist act (s.34(1) TSOFA).

Scope of liability and sanctions

132. The mental element of the TSOFA terrorist financing offences is intention, knowledge or reasonable grounds for belief. As described above in section 2.1, the law allows for these mental elements to be inferred from objective factual circumstances.

133. Criminal liability for terrorist financing extends to both natural and legal persons (see definition of "person" in s.2(1) of the Interpretation Act). Additionally, criminal liability can be vicariously extended to key officers of a legal person that has committed an FT offence unless the officer proves that the offence was committed without his consent or connivance and he had exercised reasonable due diligence to prevent the commission of the offence. Legal persons may also face parallel criminal, civil and administrative proceedings and actions in Singapore. See section 2.1 of this report for full details.

134. For terrorist financing offences under sections 3 to 5 of the TSOFA, natural persons are liable to a maximum fine of SGD 100 000 and/or imprisonment of up to 10 years, while legal persons are liable to a maximum fine of SGD 100 000. Although the potential term of imprisonment of ten years is higher than that for money laundering and other white collar offences (generally 7 years), the potential fine is significantly lower than the SGD 500 000 (natural persons) and SGD 1 000 000 (legal persons) provided for by the recent amendments to the CDSA in relation to ML. Thus, a financial institution that violates a TSOFA provision would arguably face 1/10 the fine of a similarly situated institution violated the CDSA. Singapore should consider amending the TSOFA to cross-reference the CDSA penalties, or make some other revision that would better harmonize the two statutes.

135. The prosecutorial scheme for terrorist financing offences is further complicated by the regulations to implement the UN Security Council Resolutions regarding the freezing of terrorist assets – the UN (ATM) Regs 2002 (applicable to natural and legal persons except financial institutions) and the MAS (ATM) Regs (applicable to financial institutions) which are discussed in further detail in section 2.4 of this report. Both criminalise making funds available to or dealing with property of terrorists, but carry lower penalties than those in the TSOFA – up to five years imprisonment for the UN(ATM) Regs and a fine of up to SGD 10 000 for the MAS (ATM) Regs. The AGC indicated that there are guidelines for prosecutors to determine the appropriate charging scheme. However, these guidelines were not made available to the assessment team, and because Singapore has not prosecuted any natural or legal person under any of its FT offences, the possible problems with these potentially redundant provisions cannot be assessed.

Recommendation 32 (Terrorist financing investigation/prosecution data)

Statistics and effectiveness

136. To date, Singapore has had no FT prosecutions or convictions. Although certain funds were frozen based on belief of a connection to FT activities, subsequent investigation has not yet established sufficient grounds to prosecute or obtain a final confiscation order on the funds.

2.2.2 Recommendations and Comments

137. Singapore should amend its legislation to clearly cover the financing of all terrorist acts contained in the conventions and treaties that are listed in the Annex to the FT Convention without the extra purpose requirements. Because of a lack of prosecutions, and therefore convictions, the effectiveness of Singapore's FT the provisions has not been tested and cannot be assessed. However, there is concern that the apparent overlapping of provisions in the TSOFA, the UN (ATM) Regulations and the MAS (ATM) Regulations, which provide for different penalty regimes, may negatively impact the effectiveness of the prosecutorial scheme. It is recommended that Singapore consider simplifying its framework of terrorist financing offences (*e.g.* by consolidating them into the TSOFA) in order to avoid inconsistencies and disparities in the sentencing and penalty framework.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**LC**	• Not all of the offences in the Annex to the FT Convention are terrorist acts in Singapore, an extra purpose requirement contravenes the Convention, and so financing of the Convention acts is not fully criminalised. • The effectiveness of the FT provisions has not been tested and cannot be assessed.

2.3 Confiscation, Freezing and Seizing of Proceeds of Crime (R.3)

2.3.1 Description and Analysis

Confiscation of proceeds of crime

138. Sections 4 and 5 of the CDSA permit court-ordered confiscation orders against all defendants for proceeds, or "benefits," derived from criminal conduct following the convictions of those defendants for any offence listed in the CDSA Schedules. When proving that property amounts to proceeds of crime for confiscation purposes, it is not necessary that a person be convicted of a predicate offence. Section 5(1) of the CDSA only requires a conviction for a "serious offence", which could be the money offence alone (see the Second Schedule). Section 5(2) permits confiscation of benefits from criminal conduct.

Confiscation of instrumentalities

139. The CDSA does not address the confiscation of any property which constitutes the instrumentalities used in, or intended for use in, the commission of drug trafficking or a serious crime. However, for domestic investigations, the police may use the restraint and confiscation provisions under the Criminal Procedure Code (CPC). Section 386 of the CPC permits a court to order forfeiture or confiscation of any property "regarding which any offence is or was alleged to have been committed or which appears to have been used for the commission of any offence," regardless of whether a conviction is obtained, during or at the conclusion of a Singapore investigation or trial. The Singapore police agencies all confirmed that they use section 386 widely to confiscate the assets seized during the course of an investigation, including the instrumentalities of crime, often even without a conviction being obtained.

140. In addition, the Misuse of Drugs Act (MDA) provides for the forfeiture of controlled substances and drug paraphernalia (s.27, also not requiring a conviction), and of vehicles and other modes of transportation which facilitated the drug trafficking (s.28, requiring a conviction). The CNB confirmed that over 130 of their confiscations in drug investigations (primarily vehicles and currency) were accomplished under section 386, while they used the section 4 CDSA confiscation authority less frequently. The CPIB conducts most of their confiscations under section 13 of Prevention of Corruption Act.

Property subject to confiscation

141. Parts II, III and IV of the CDSA adequately provide for the restraint and confiscation of "benefits derived" by a convicted defendant from drug trafficking (s.4) or criminal conduct constituting a serious offence listed in the Second Schedule of the CDSA (s.5) (which includes the ML offences codified in sections 44 and 47). Sections 4(4) and 5(6) of the CDSA contain rebuttable presumptions that, if a person holds or has *at any time* held any property or interest in property that is disproportionate to his/her known sources of income, the holding of which cannot be explained to the satisfaction of the court, such property or interest shall be presumed to be benefits derived from such offences. These presumptions may operate regardless of where the proceeds come from, as long as they were derived from a predicate offence (ss.4(5) and 5(8) CDSA).

142. Singapore law permits the court to order actual confiscation of only "realizable property," defined in section 2(1) of the CDSA as property that is held by a defendant and property gifted directly or indirectly by one defendant to another. However, if a prosecutor learns that the defendant subsequently acquires additional property, the court may increase the confiscation order by that amount, including any substitute property (s.10(6). "Property" is defined as money and all other property, movable or immovable, including things in action and other intangible or incorporeal property, situated in Singapore or elsewhere, while "interest", in relation to property, includes any right.

143. The Singapore authorities state that property is still considered held by the defendant if he/she holds any interest in it (including a beneficial interest), even if the property is held by a third party by virtue of the wide definition of "property". However, under the CDSA, property held by third parties is subject to confiscation only if it was gifted by the convicted defendant: (1) within six years prior to commencement of the criminal case, or (2) at any time if the gift was of criminal proceeds (section 16(1) read with sections 12(7) and 12(8), CDSA). Under s 13(2) CDSA, a person can apply to court to declare his interest if:

(a) He was not in any way involved in the defendant's drug trafficking or criminal conduct, as the case may be.

(b) He acquired the interest –

  (i) For sufficient consideration.

  (ii) Without knowing, and in circumstances such as not to arouse a reasonable suspicion, that the property was, at the time he acquired it, property that was involved in or derived from drug trafficking or criminal conduct, as the case may be**.**

144. Thus, only a person who was not involved in the defendant's criminal conduct and who acquired the interest for sufficient consideration and without knowledge or reasonable suspicion of the illicit origins of the property will be able to obtain the court's protection of his interest in the property.

Provisional measures

145. Authorities generally use the CPC to provisionally seize property. Section 68 authorises authorities to provisionally seize "any property which is alleged or suspected of having been stolen or which is found under circumstances which create suspicion of the commission of any criminal offence." The police often use this provision in the first instance because, unlike the CDSA, it does not have the prerequisite of criminal proceedings being initiated or the defendant being advised that criminal proceedings will ensue. However, the CPC provisions only apply to the seizure of items constituting evidence of a crime which might be used to prove the elements of the offence. This does not clearly capture all instrumentalities and intended instrumentalities of crime or "substitute property" for instrumentalities, as is required by Recommendation 3. Apart from section 68 of the CPC, there are also other provisions under Singaporean law that can apply to the restraint of instrumentalities or intended instrumentalities of predicate offences, such as: section 11(1)(a) read with sections 24(1) and 21(b) of the TSOFA and section 24(1)(c) of the MDA; section 138(s)(b) of the Copyright Act; sections 14(2)(d), 15 and 16 of the Strategic Goods (Control) Act; section 28(1) of the Societies Act; and section 11(3) of the Betting Act.

146. In addition to the above provisions, sections 15 and 16 of the CDSA empower the High Court to issue a restraint order for property that may become the subject of a confiscation order upon conviction. The restraint order may be issued *ex parte* (s.16(4)(b) CDSA), but only after actual criminal proceedings have been instituted, or a defendant has been informed that he/she may be prosecuted for a predicate offence (s.15(2) CDSA). Singapore generally employs section 68 of the CPC to prevent asset depletion at a very early stage of investigations even before a defendant is informed that he or she may be prosecuted. Following such seizure, restraint orders under CDSA are usually applied for when there are third-party interests involved. Such orders generally prohibit any person from dealing with, transferring or disposing of any realisable property and, in making such an order, the High Court can also appoint a receiver to take possession of and manage the property in question. Upon the making of a restraint order, the property may be seized and be dealt with in accordance with the directions of the High Court. A restraint order may be discharged or varied in relation to any property, and shall be discharged when the proceedings for the predicate offence are concluded (s.16 CDSA).

147. Charging orders can be made in respect of any interest in "realisable property" that is in the form of immovable property (land), specific types of securities or under any trust for the purpose of securing payment to the government either an amount equal to the value from time to time of the property charged or an amount not exceeding the amount payable under the confiscation order. A charging order may be discharged or varied, and shall be discharged when the proceedings for the predicate offence are concluded or when the amount secured by the charge is paid into court (s.17 CDSA).

148. The CDSA does not provide for a restraint of instrumentalities or intended instrumentalities of predicate criminal offences.

149. Restraint orders under both the CDSA and the CPC may be made on an *ex parte* application to a judge in chambers, as long as the orders provide for subsequent notice to be given to persons affected by the order (s.16(4) CDSA).

Powers to trace property and protection of rights

150. Singapore law enforcement agencies (such as the CNB, CPIB, CAD and SPF, and officers of the FIU – STRO), and public prosecutors have powers to identify and trace property that may become subject to confiscation. Part V of the CDSA contains specific provisions for obtaining production orders seeking unprivileged information that is material to an investigation into drug trafficking or serious criminal offences. However, a dual standard applies which is not commonly observed in AML/CFT statutory schemes.

151. Section 30 of the CDSA permits police officers investigating either drug trafficking or criminal conduct to directly obtain from "a court" material that may be of substantial value to the investigation. Section 35(2) clarifies that "court" means High Court and District Court. However, section 30 expressly does not permit the same procedure with regard to material maintained by a financial institution. Section 31 provides that only the Attorney General (or a written delegate) may apply only to the High Court for information that is needed for an investigation and which is in the possession of a financial institution, and such information must be produced to the Attorney General (not to the police). This added layer of required approvals and restrictions surrounding the obtaining of bank information (as opposed to *any other* relevant information), though not exactly a bank secrecy provision, may, at times, prove dilatory and onerous to an investigation. The Attorney General may also seek an order from the High Court permitting disclosure of information held by public bodies for investigative purposes (s.42 CDSA).

152. Singapore law enforcement agencies and the AGC confirmed that the police often use section 58 of the CPC to obtain information relevant to their investigations. Section 58 authorises officers to directly obtain the production of the relevant evidence. Again, bank information is treated differently, requiring the participation of an officer of inspector level or higher. According to Singapore authorities, this power can be used to compel the production of customer identification materials and account opening records to identify and trace property that is subject to confiscation or is of suspect origin. Law enforcement officers indicated that they have no problems using this provision to obtain bank records and this was also accepted by the financial institutions. Customs officers and other officers who are not members of the SPF have CPC powers when they are investigating offences under the CDSA (s.55 CDSA).

153. A person who asserts an interest in property, which is the subject matter of application for a confiscation order, may apply to the court for an order declaring the nature, extent and value (as at the time the order is made) of that person's interest (s.13 CDSA). The applicant may defeat the forfeiture if he/she satisfies the court that he/she: (1) was not in any way involved in the criminal conduct; *and* (2) that he/she acquired the interest for sufficient consideration and without knowing (and in circumstances such as not to arouse a reasonable suspicion) that the property was, at the time the interest was acquired, property that was involved in or derived from drug trafficking or criminal conduct (s.13(2) CDSA).

154. According to Singapore authorities, the general principle that illegal contracts are unenforceable, regardless of whether the transactions are prohibited by statutes or deemed illegal by judicial precedents (including contracts against public policy or contracts to commit torts or criminal acts), should permit a voiding of such transfers of or agreements to transfer property. The CDSA specifically provides for the voiding of gift transfers which: (1) occurred with the prior 6 years (for legitimate property); or (2) occurred at any time in the case of criminally-derived property.

Additional elements

155. The Singapore authorities indicate that the property of criminal organisations could be confiscated by charging the criminal organization under the conspiracy provisions of the Penal Code and then using that as the basis to confiscate criminally-related property. However, this has not been tested. As well, a procedure analogous to confiscation under the Societies Act could be applied to a registered society that is subject to dissolution, having been used for unlawful purposes or for purposes prejudicial to public peace, welfare or good order in Singapore (s.24(1). Upon dissolution all of a society's property vests in an appointed Receiver (s.25).

156. Singapore does not have a civil confiscation regime. However, Singapore authorities contend that the dissolution procedure for "unlawful societies" is analogous to a civil forfeiture in that the society's assets are confiscated without the conviction of any person. In addition, section 386 of the CPC provides for general court jurisdiction to forfeit some criminally-related property at the conclusion of a criminal case, without specifying that a conviction must be obtained. This latter procedure is, however, wholly at the court's discretion, and there are no guidelines set forth as to how the court should determine forfeitability or how to measure third party interests.

157. As noted above, Singapore has a rebuttable presumption requiring a convicted defendant to demonstrate, on a balance of probabilities, the lawful origin of property subject to confiscation (ss.4(4) and 5(6) CDSA).

Recommendation 32 (Confiscation/freezing data)

Statistics and effectiveness

158. The relevant law enforcement agencies keep statistics on the amounts of property frozen, seized, returned and confiscated in relation to ML and FT. For predicate offences in relation to white collar crimes (including cheating, criminal breach of trust and forgery), the CAD is responsible for keeping such statistics. The FIB maintains the relevant statistics in relation to terrorist financing. For predicate offences involving drug and corruption matters, this responsibility rests with CNB and CPIB respectively.

159. The following chart sets out the statistics for the amount of number of cases in which freezing/seizing orders, confiscation orders and forfeiture orders were made between 2004 and 2007 (as of 14 November 2007) pursuant to both predicate offence and related money laundering investigations.

	2004	**2005**	**2006**	**2007 (14 Nov 2007)**
Number of Cases in which Freezing/Seizing Order was Made	173	182	274	325
Number of Confiscation Order pursuant to CDSA	7	1	1	1
Number of Other Forfeiture Orders	75	45	39	30

160. The chart below shows a consolidated overview of the total amount of monies frozen/seized, forfeited and confiscated by Singapore from 2004 to 2007 (as of14 November), in relation to predicate offences and related money laundering. These figures all relate to the investigation and prosecution of domestic predicate offences relating to money laundering. The statistics also show that monies frozen during investigations are being restituted to the victims of the crime at the conclusion of the investigation/criminal trial. For example, the monies restituted in 2007 are mainly from monies frozen in 2004 as time is needed for the conclusion of the case, including the court trial and the disposal of the assets to the victims of the crime.

Monies Frozen, Forfeited or Confiscated, and Restituted relating to all Domestic Predicate Offences

	2004	**2005**	**2006**	**2007 (14 Nov 2007)**
Amount Frozen / Seized	SGD 8 379 675 (EUR 3 936 771)	SGD 23 941 436 (EUR 11 245 292)	SGD 15 608 908 (EUR 7 333 064)	SGD 7 218 338 (EUR 3 389 050)
	USD 360 038 (EUR 245 005)	USD 1 500 303 (EUR 1 020 956)	USD 211 119 (EUR 143 666)	USD 3 464 978 (EUR 2 358 250)
	AUD 130 000 (EUR 78 455)			MYR 54 040 (EUR 10 900)
				EUR 3 271 317
				CHF 134 462 (EUR 84 333)
Total frozen/seized	**EUR 4 260 231**	**EUR 12 266 248**	**EUR 7 476 730**	**EUR 9 113 850**
Amount Forfeited / Confiscated*	SGD 1 776 265 (EUR 833 956)	SGD 3 107 132 (EUR 1 459 109)	SGD 2 030 265 (EUR 953 412)	SGD 768 217 (EUR 360 682)
Amount Restituted	SGD 10 997 (EUR 5 161)	-	-	SGD 5 743 555 (EUR 2 696 631)
				USD 814 389 (EUR 554 191)
Total forfeited / confiscated or restituted	**EUR 839 117**	**EUR 1 459 109**	**EUR 953 412**	**EUR 3 611 504**

*This figure includes monies that are being paid by way of penalty under section 13 of the Prevention of Corruption Act. The amount paid would be the equivalent of the amount of gratification as ordered by the Court.

161. Attached in the table below is the total amount of monies frozen pursuant to cases involving foreign predicate offences, which includes Singapore domestic investigations and seizures at the request of foreign governments, based on foreign investigations. Such cases would also typically result in assistance being rendered to a foreign jurisdiction. The figures are also indicative of Singapore's enforcement efforts in investigating money laundering offences not related to a domestic predicate offence, and general co-operation or acting in response to foreign requests for assistance.

Monies Frozen, Restituted Relating to Money Laundering related to Foreign Predicate Offences

	2004	2005	2006	2007 (as at 14 Nov)
Number of ML Cases involving foreign predicate offences	2	3	2	14
Amount Frozen / Seized	-	-	SGD 1 505 626 (EUR 706 899)	SGD 7 110 000 (EUR 3 338 184)
	-	USD 200 000 (EUR 136 119)	USD 6 231 859 (EUR 4 241 379)	USD 220 457 (EUR 150 042)
	-	EUR 100 000		EUR 47 500 000
	-	GBP 100 000 (EUR 133 890)		
Amount Restituted	SGD34 850 (EUR 16 362)	-	-	-

162. The statistics show a comprehensive record listing the assets frozen, seized for investigation, confiscated, forfeited and realized with regard to the offences listed under CDSA, including predicate offences and money laundering. However, as noted above, separate statistics are not kept of the amounts frozen in relation to specific types of offences (*e.g.* predicate offences or ML). Statistics that are kept by individual law enforcement agencies which are responsible for investigating specific types of crimes give some additional clarity. For instance, the chart below sets out the amounts frozen/seized and confiscated by the CNB which is responsible for investigating drug offences – meaning that the CNB statistics relate to drug offences and related money laundering.

Specific breakdown of CNB's statistics in relation to drug offences and related money laundering

Year	No. of Cases	Amount Frozen/Seized	No. of CDSA Confiscations	Other Forfeiture	Total Confiscated (SGD)
2004	170	SGD 604 389 / (EUR 283 881)	7	75	SGD 410 282 / (EUR 192 708)
2005	179	SGD 444 330 / (EUR 208 701)	1	45	SGD 136 399 / (EUR 64 066)
2006	261	SGD 4 156 607 / (EUR 1 952 773)	1	39	SGD 147 121 / (EUR 69 102)
2007 (14 Nov)	298	SGD 773 443 / (EUR 363 135)	1	30	SGD 99 197 / (EUR 46 573)

163. However, even the statistics from individual law enforcement agencies (such as the CNB) are not broken down to show whether assets have been frozen in relation to a drug (predicate) offence or drug-related money laundering. The Singapore authorities explain that, in general, their statistics do not specifically distinguish between cases in which there is a close relation between the domestic predicate offences and the money laundering investigations. In other words, when a seizure is made in relation to a financial investigation resulting from a domestic predicate offence, the seizure will be regarded as both for money laundering as well as for the domestic predicate offence

164. Overall, given the risk of money being laundered in Singapore (particularly the proceeds of foreign predicate offences), the amount of money being frozen and seized seems low. Between 2004 and the end of 14 November, the authorities froze/seized approximately EUR 89 273 530.

2.3.2 Recommendations and Comments

165. Singapore should extend its restraint provisions to all instrumentalities and intended instrumentalities of crime, and "substitute property" for instrumentalities. Additionally, Singapore should consider amending the provisional restraint provisions under the CDSA to ensure that restraint may occur before a defendant is charged or informed that he/she will be charged, to avoid running the risk that assets will be depleted before they can be seized.

166. Singapore should more actively pursue confiscation of frozen/seized assets. It should also streamline the procedure for obtaining bank records (by High Court order through application by the AGC) which is cumbersome compared to the procedure by which the police may simply seek a court order directly (*i.e.* without going through the AG) from either the High Court or District Court to obtain all other information.

167. It does not appear that restraining or forfeiture orders, for predicate crimes in particular, are generally pursued under the CDSA at all. Much of the confiscated property reported by Singapore (especially in drug cases) appears to have occurred under the CPC's general police powers. The authorities should consider whether using CPC's general powers for restraining property, rather than the existing powers in the CDSA, could present any future problems for retraining property relating to ML.

168. Singapore should also ensure that its statistics distinguish between cases involving freezing/seizure and confiscation for ML and for predicate offences.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**LC**	• The restraint provisions do not extend to property of corresponding value, and it is unclear whether restraint provisions extend to all instrumentalities and intended instrumentalities of crime. • Effectiveness: Given the risk of money being laundered in Singapore (particularly the proceeds of foreign predicate offences), the amount of money being frozen and seized seems low. The procedure for obtaining bank records (by High Court order through application by the AGC) is cumbersome compared to the procedure by which the police may simply seek a court order directly (*i.e.* without going through the AG) from either the High Court or District Court to obtain all other information – without any apparent reason to differentiate between the two types of evidence.

2.4 Freezing of Funds Used for Terrorist Financing (SR.III)

2.4.1 Description and Analysis

Basic legal framework for freezing terrorist-related assets

169. The basic provisions to prevent financial institutions and other persons from dealing with terrorist-related assets are contained in the UN (ATM) Regulations s (s.6), which indicate that no person in Singapore shall:

> "a) Deal, directly or indirectly, in any property that he knows or has reasonable grounds to believe is owned or controlled by or on behalf of 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 person referred to in paragraph (a) to, or for the benefit of, or on the direction or order of, any terrorist or terrorist entity."

170. The definition of "terrorist" is defined as any person who commits, attempts to commit, participates in or facilitates the commission of any terrorist act, and specifically includes any person referred to in the Schedule, which makes reference to all entities belonging to or associated with the Taliban and Al Qaida pursuant to the 1267 List.

171. Prohibitions on financial dealings contained in section 6 of TSOFA mirror the language of and also make reference to the Schedule of the UN (ATM) Regulations. Failure to comply is a criminal offence punishable by up to SGD 100 000 or to imprisonment up to ten years or both. Identical language is also found in section 6 of the MAS (ATM) Regulations, with the exception that the prohibition explicitly applies to "financial institutions." The Schedule to the MAS (ATM) Regulations is the same as for the UN (ATM) Regulations.

Laws and procedures to freeze pursuant to S/RES/1267(1999)

172. When the UN Al-Qaida and Taliban Sanctions Committee (the 1267 Committee) designates a person or entity pursuant to S/RES/1267(1999), Singapore's UN Mission in New York transmits the designations to the Ministry of Foreign Affairs (MFA) which, in turn, transmits them to the relevant government ministries and agencies (*e.g.* the MAS, MHA, the MinLaw, the Ministry of Finance and the Ministry of National Development). When the UN amends the list, this is automatically included in the Schedules (s.1(c), Schedules of the UN(ATM) Regulations and the MAS(ATM) Regulations). Additions and updates are effective immediately upon their inclusion in the 1267 list, taking into account the 12-hour time difference between Singapore and New York.

173. Upon receipt of a designation, the respective Ministry directs its respective agencies to take appropriate action by screening their databases. MAS distributes the information to financial institutions pursuant to the MAS (ATM) Regulations. The respective Ministry will inform the non-financial regulatory boards (*e.g.* Accounting and Corporate Regulatory Authority (ACRA), the Central Provident Fund (CPF), the Housing Development Board (HDB), Land Transport Authority (LTA), and Singapore Land Authority (SLA). Those agencies, in turn, will conduct database checks to determine whether the designated persons or entities own any real estate, corporate interests, or other assets in Singapore.

174. MAS advises the FIs of updates to the UNSCR 1267 list. The MAS circulates the designation information that it receives to all financial institutions in Singapore when MAS issues announcements on its website. A link to the UN website is provided on the MAS website. Pursuant to its regulatory authority, MAS has issued the MAS (ATM) Regulations pertaining to FT funds, and has a link on its website to the 1267 listed entities. In such cases, the FI must comply with the direction or regulation notwithstanding any other duty imposed by any rule of law, written law or contract (s.27A, Monetary Authority of Singapore Act (MAS Act). Any financial institution that fails (or refuses to) comply with a direction issued to it, contravenes any regulations, or discloses a direction issued to it is guilty of an offence. All regulated sectors met with by the assessment team confirmed that they receive the updates from MAS.

175. Financial institutions are required to report to MAS if they have any financial transactions, including bank accounts, with any designated persons or entities (s.9 MAS (ATM) Regulations). Similarly, all persons are required to report to the Commissioner of Police if they are in possession, custody or control of any terrorist-related property or have information about any transaction or proposed transaction in respect to terrorist-related property (s.10 UN (ATM) Regulations; s.8 TSOFA). Such reporting may be done via a police report and through filing an STR with the STRO. The MAS (ATM) Regulations and UN (ATM) Regulations prohibit regulated FIs and DNFPBs from accepting, or "dealing in," funds which they believe may be terrorist-related without the prior written approval of the MAS (ss.5 and 6, MAS (ATM) Regs). The effect of these provisions is that property is temporarily frozen until the FI receives further instructions from CAD.

176. Those who make disclosures to the Commissioner of Police in good faith are immune from criminal or civil proceedings for such disclosure. While there is no specific tip-off provision for actions conducted under the authority of TSOFA itself, the terrorism financing offences under the TSOFA are 'serious offences' under the Second Schedule of the CDSA, and section 39 of the CDSA requires anyone who knows or has reasonable grounds to suspect that any property is linked to such offences to lodge an STR. In addition, it is an offence for any person with knowledge that an investigation for the purposes of the CDSA (including for predicate offences) is taking place or about to take place to make any disclosure likely to prejudice the investigation (s.48(1) CDSA). This tipping-off provision does not fully cover the situation of someone in the process of filing an STR, but covers the past act of having filed one. The Singaporean authorities have indicated that they have addressed that gap with the enactment of a new offence of obstructing the course of justice which has recently been passed, but is not yet effective (s.204A Penal Code (Amendment) Act 2007).[17]

177. The financial sector representatives interviewed by the assessment team indicated that they know that they are to contact the CAD with any such terrorist financing-related information. Several DNFBPs and money remitters indicated that they believed they could simply refuse to accept any funds which they believed to be terrorist-related, or related to any of the entities designated on the 1267 list. In such cases, CAD would usually be contacted for advice, and a STR reported at the least. These representatives confirmed that CAD conducted frequent outreach to the community to update on procedures for detecting and freezing terrorist and terrorist-related property, and they knew that CAD conducted a Hotline for the purpose of receiving any relevant information.

178. The MAS (ATM) Regulations require all financial institutions in Singapore to immediately and automatically freeze all assets belonging to or controlled by S/RES/1267(1999) persons and entities within their possession. Thus, if funds are in the possession of the financial institution, there is no requirement under the Regulations for a court order to be sought and obtained by the AGC in order for a freeze to occur. This automatic freeze finds it basis in MAS Regulations 6 and 7 prohibiting institutions from dealing with such assets without the prior written approval of MAS. The effect of these provisions is that the funds of such designated persons or entities are, for all intents and purposes, frozen. The TSOFA also contains provisions for freezing and restraining property (ss.11(a) and (b), pursuant to an order made by the High Court, but such an order is only necessary when the property is in the hands of third parties, or is sought to be forfeited eventually.

179. There are procedural rules governing applications made under Part IV of TSOFA (Order 89E, Rules of Court (ROC). A TSOFA restraining order, issued under the authority of section 11 of TSOFA may be made on an application by the AGC that must be supported by an affidavit which states the grounds for believing that the property is owned by, or controlled by, a terrorist or terrorist entity, or has been or will be used to facilitate a terrorist act. These grounds may be based on information received; personal knowledge is not required. The application must also state the "full particulars and the location of the property" sought to be restrained, and the person or persons in possession of the property (Order 89E Rule 2(3), ROC). However, no mention needs to be made of the designated person or entity, and no person may inspect or take a copy of any document filed in support of such an order without leave of a judge. The AGC must serve copies of the order on the "defendant" and on all parties "affected by the order." Such an order is available if the AGC has shown that there is sufficient evidence to establish that the property belongs to or is controlled by or on behalf of a terrorist organization, or that the property was used or is intended for use in committing a terrorist act, whether locally or overseas (s.21 TSOFA). In both cases, the enforcement authority (*e.g.* FIB) would have to assess whether there are sufficient facts to request the Attorney-General to make an ex-parte application to search, seize or restrain the assets of the suspected terrorist financier. Before restraining

[17] This provision will supplement the tipping-off offence in the CDSA, and will cover all disclosures made pursuant to the provisions of TSOFA, and provides as follows:

"Obstructing, preventing, perverting or defeating course of justice

204A. Whoever intentionally obstructs, prevents, perverts or defeats the course of justice shall be punished with imprisonment for a term which may extend to 7 years, or with fine, or with both."

the property, the court may require the AGC to take some action with regard to indemnifying potential property loss (s.13 TSOFA). A TSOFA seizure or restraining order extends for only six months, unless further extended by the issuing court. As Singapore has never utilized the TSOFA procedure for freezing terrorist-related property, the efficiency and speed of this procedure has not been tested.

180. The parallel UN (ATM) Regulations 2001 apply to all persons and entities in Singapore (other than financial institutions) and impose a similar automatic asset freeze on all property owned or controlled by designated terrorists and terrorist organizations, including all persons/entities on the 1267 List and persons/entities coming under the ambit of UNSCR 1373. Non-financial institution entities indicated to the assessment team that they were aware of the 1267 designations, received notices in this regard from the CAD on a regular basis, knew of their obligation to report any attempted transactions by such entities immediately to the CAD, and understood that the CAD would inform them further of their obligations with respect to the property.

Laws and measures to freeze pursuant to S/RES/1373(2001)

181. The MAS (ATM) Regulations and the UN (ATM) Regulations, likewise, govern the implementation of S/RES/1373(2001), in a potentially two-track fashion. Singapore has articulated a procedure by which it may designate its own list of terrorists or terrorist entities to give recognition to those designated by other countries, but it has not utilized this procedure. Instead, Singapore has taken another option, on several occasions, of freezing the funds of such entities at the request of foreign governments using its general police powers (CPC), with governing provisions of the TSOFA.

182. Singapore contends that because the UN (ATM) and MAS (ATM) Regulations have defined the term "terrorist" as any person who commits or attempts to commit any terrorist act or participates *in or* facilitates the commission of any terrorist act, and because the term "terrorist act" is defined broadly to cover every conceivable terrorist act, the Regulations also govern any terrorist person or entity designated by any country pursuant to S/RES/1373(2001). Thus, beginning in 2001, Singapore has successfully identified and frozen the assets of a number of terrorist individuals and organizations (none on the 1267 List), and without a separate internal designation of its own terrorist list. Thus, while Singapore has not, itself, made any designations pursuant to S/RES/1373(2001), it has implemented its own domestic procedures to allow the country to block assets owned and/or controlled by individuals or entities designated by other countries. The first procedure (an internal designation of its own separate list) appears entirely viable, but has not been tested, so its effectiveness cannot be evaluated. However, the second procedure has been successfully applied multiple times beginning in 2001 and up through 2007.

183. Although there is not an explicit recognition as such, Singapore regards a domestic designation of terrorists and/or terrorist organizations as within the portfolio of the MHA. More importantly, even without a domestic designation, Singapore can respond to requests from other countries that have made such designations by blocking assets. Thus, in situations where the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, Singapore will ensure that the funds or other assets of the designated person are frozen without delay.

184. To date, on occasions when Singapore has determined to block assets belonging to terrorist organizations designated pursuant to S/RES/1373, the MHA (IMC – Terrorist Committee) considered the quality and specificity of the information provided by the other countries. In these cases, Singapore requires that countries provide sufficient evidence that is supported by reasonable grounds. Again, although Singapore has not specified the "legal grounds" for making those determinations, by demonstrating results in several cases, it maintains a viable internal agency mechanism through which reliable determinations are made. The net result is that the government of Singapore, and most of its major financial institutions, check many such lists (*e.g.* the OFAC list) and designations by other countries, and where appropriate, effect regulatory freeze, referral to CAD, CPC seizure authority, and possibly eventual use of TSOFA for seizure, restraint and/or forfeiture. These procedures have worked

for Singapore in the context of certain S/RES/1373(2001) designations, even though they are not clearly delineated by regulation and statute.

185. MAS has instructed its regulated institutions to work with CAD. In practice, they would effect a temporary freeze (*e.g.* 24 hours) which is sufficient to permit a reporting to the CAD, and for a determination to be made as to whether to obtain a more permanent freeze, or a seizure of the property under section 68 of the CPC. The financial institutions whom the assessors interviewed in Singapore also confirmed that, pursuant to their governing regulations, training by MAS, and (for some international banks) their internal policies, they would enact a provisional freeze on suspected terrorist or terrorist organization-related funds about which they had received information (either internally from lists kept by international institution headquarters or from CAD or some other Singapore official agency). The assessment team was provided with examples of assets which were frozen or seized beginning in 2001 belonging to suspected individual members of Jemaah Islamiyah, a 1267-designated organization, through an exercise of the CAD police powers. Subsequently, the MHA exercised its authority under provisions of TSOFA (specifically s.7(1) to exempt certain of the seized/restrained JI properties as necessary for the living expenses or other necessities of certain individuals from the mandated freeze provisions of TSOFA section 6. These exemption orders were published in the Government Gazette throughout 2005, 2006 and 2007.

186. Singapore, may, of course, as an alternative, also use the formal mutual legal assistance process at the request of a foreign government (s.29(1)(b) MACMA) or the TSOFA section 11 court-ordered procedure, absent any criminal proceedings at home or abroad, in order to proceed against suspected assets within its borders, at the request of a foreign government, as well as the automatic freezing regime laid down by the UN (ATM) Regulations and the parallel MAS (ATM) Regulations. However, this would be an unduly lengthy procedure that would not permit the expedient freezing of terrorist-related assets without delay and without prior notice to the designated persons involved. The formal mutual legal assistance process is described in section 6.3 of this report.

187. Singapore has also used its regulatory scheme and general police powers, as described above, to accede to requests by foreign governments, after examining the quality and specificity of evidence provided, to freeze funds during 2004 (SGD 13 549), 2005 (SGD 17 883), 2006 (SGD 21 859), and 2007 (as at 14 November) (GBP 209, SGD 4 467).

Guidance

188. The MAS (ATM) Regs give guidance to financial institutions on how to give effect to S/RES/1267(1999), S/RES/1373(2001) and S/RES/1333(2000), and S/RES/1390(2002). These Regulations apply to the Singapore branches and offices of financial institutions that are incorporated outside Singapore but operate within Singapore, and to all branches and offices (wherever located) of financial institutions incorporated in Singapore. Similar guidance is contained in the UN (ATM) Regs which apply to non-financial institutions.

189. Both sets of regulations impose obligations to report and cooperate with the authorities. For instance, a financial institution that finds that it has possession, custody or control of any property belonging to any terrorist or entity owned or controlled by any terrorist, and requirements must immediately inform the MAS (or its designate) and to provide further information concerning the property, transaction or proposed transaction as required (s.9 MAS (ATM) Regs). Similar obligations apply to NFIs which must immediately report to the Commissioner of Police (or its designate) (s.10 UN (ATM) Regs).

Procedures for delisting, unfreezing and obtaining access to frozen funds

190. In Singapore, 1267 de-listings are effected automatically because the Schedules to the UN and MAS (ATM) Regulations incorporate the 1267 List (as amended by the 1267 Committee from time to time) automatically by reference. To date, no person or entity, other than those on the 1267 List, has

been listed in the Schedules. However, the Singapore authorities have explained that if such a person or entity were to be listed (pursuant to a domestic 1373 listing) in the Schedules, delisting can be effected easily, by amending the relevant entry in the Schedules via Gazette Notification to remove the name from the list maintained by MHA.

191. Section 19 of TSOFA contains specific procedures for unfreezing the funds or other assets of persons or entities, for humanitarian purposes, which were affected by a freezing order. Any person who has an interest in a property seized or restrained under section 11(1) of TSOFA may at any time apply to a High Court judge for an order to return the seized property, or revoke or vary the restraint order (s.19(1)(a). Section 6(b) explicitly covers exemptions for individuals not complicit in any terrorist or terrorist financing activity.

192. TSOFA also contains procedures to authorize access to funds or other assets that were frozen and have been determined to be necessary for basic living or medical expenses, the payment of certain types of fees, expenses and service charges or for extraordinary expenses (*e.g.* reasonable living, business and legal expenses). This has been tested effectively in Singapore. The relevant agencies can obtain exemption orders under the TSOFA, and the UN (ATM) and MAS (ATM) Regulations. The court may also order property sold with the net proceeds from the sale of the terrorist's property being deposited into the beneficiary's designated bank account to receive and make withdrawals for the basic expenses allowed under S/RES/1452(2002). Furthermore, the withdrawals and the bank accounts are subject to routine inspection by the relevant authority. Persons affected by a warrant or restraint order may also apply for the return of seized property, or the revocation or variation of a restraint order, or have a warrant or restraint order made subject to reasonable conditions (s.19(4)(c) TSOFA). The Judge must however be satisfied that the applicant has no other assets or means available for any of these purposes and that no other person appears to have lawful ownership or possession of the property (s.19(5) TSOFA).

193. Although the provisions of the TSOFA, and the UN and MAS (ATM) Regulations do not expressly mention notifying and obtaining the approval of the 1267 Committee, Singapore takes the position that its international obligations require the government of Singapore to notify and obtain the approval of the UN 1267 Committee for the release of funds frozen pursuant to S/RES/1267 (1999). Singaporean authorities indicate that a law is not required to obtain 1267 Committee approval and it will, as a matter of course, not act in breach of its international obligations. Singapore indicated that any application under TSOFA for a release of such funds, and any administrative order promulgated by MHA to release funds, will be submitted to the Committee for approval prior to its filing or publication. Funds of 1267 entities frozen pursuant to the automatic asset freeze in the UN and MAS Regulations may be released by the government, via Gazette Order, once the 1267 Committee's approval has been obtained, without the requirement of a court order. In the event that the funds of a 1267 entity are frozen via court order under TSOFA with a view to forfeiture, the judge hearing the application will be informed of Singapore's international obligation to notify the 1267 Committee and obtain its approval. Any court order made under the TSOFA would have to take into account Singapore's international obligations. Notice of any release of funds frozen pursuant to S/RES/1373(2001) or as a response to another government's request, need not be submitted to the 1267 Committee as there is no requirement to do so. The government has released funds frozen pursuant to S/RES 1373(2001) if such release, on humanitarian grounds, is in accordance with the criteria set out in S/RES/1452(2002).

Freezing, seizing and confiscation in other circumstances

194. The freezing, seizure, and forfeiture of terrorist-related property can also occur outside of the UNSCR-listing contexts in Singapore through the general application of TSOFA. Such property covers funds or other assets wholly or jointly owned or controlled, directly or indirectly, by designated persons ("terrorist" as defined in TSOFA covers such persons), terrorists, and those who finance terrorism or terrorist organizations. It also includes funds derived from funds or other assets owned or controlled directly or indirectly by such persons (s.21(b) and 6(1)(a) TSOFA). However, again, a court

order is required for restraint, and confiscation will be ordered, without the requirement of a conviction, with a judicial conclusion that the property is property of terrorists based upon a standard of balance of probabilities (s.24 TSOFA).

195. "Property" is defined very widely in s 2(1) of the TSOFA to include assets of every kind whether tangible or intangible and whether movable or immovable. Thus, a terrorist's interest in jointly-owned property is also "property" that may be the subject of a freezing and a forfeiture order. In cases where such property is mixed, the order of forfeiture shall relate only to the portion owned or controlled by the terrorist or terrorist entity, based on s 24(2) of the TSOFA. As such, jointly owned property falls within the ambit of the freezing and forfeiture regime of the TSOFA; however, only the terrorist's interest is subject to confiscation. Property belonging to or controlled by persons "who finance terrorism or terrorist organisations" can be forfeited so long as it falls within section 21(b) of the TSOFA. Under s 21(b) of the TSOFA, property that has been or will be used in whole or in part to facilitate or to carry out a terrorist act may be subject to an order of forfeiture upon the application of the AG to the High Court, and may occur in the absence of any criminal conviction. If the Court is satisfied "on a balance of probabilities" that the government has made the necessary showing, forfeiture will be ordered of the terrorist's interest.

196. If in the course of facilitating or carrying out a terrorist act, a serious offence which is a predicate offence in the Second Schedule of the CDSA is also committed, restraint and confiscation is possible under the mechanism of the CDSA, in respect of benefits derived from such criminal conduct. And, of course, as always, law enforcement officers may use their general powers under the CPC to search or seize any asset belonging to a suspected terrorist financier in "circumstances which create suspicion of the commission of any offence" (including FT offences) (s.68(1) CPC), and may forfeit such property (s.386 CPC) ("any property regarding which any offense is or was alleged to have been committed or which appears to have been used for the commission of any offense"). This provision has been used since 1992 and there has never been a challenge on this basis.

Protection of third parties

197. TSOFA has a number of safeguard provisions that protect the rights of innocent third parties acting in good faith. For instance, the judge may require undertakings from the Attorney-General with respect to the payment of damages or costs for the warrant or seizure order (s.13 TSOFA). Likewise, appropriate compensation may be ordered by the High Court against an innocent third party if the person is aggrieved or prejudiced by an improper investigation against him (s.50 CDSA). TSOFA provides, essentially, an "innocent owner" defence applicable to property sought for forfeiture under these provisions (s.26 TSOFA).

198. In the case of an application to forfeit property under section 21 TSOFA, the Attorney-General is required to give notice of the intended application to persons who are known to own or control the property (s.23 TSOFA). This extends to persons who, in the opinion of the judge, appears to have interest in the property (s.23(3) TSOFA). The claimant of an interest in forfeited property who did not receive such notice may apply to a judge to vary or set aside the forfeiture order not later than 60 days after its making (s.27(1) TSOFA). In addition, there is a mechanism by which a person or entity whose funds or other assets have been frozen may challenge the measure with a view to having that challenge reviewed by a court (s.19(1) TSOFA).

199. A judge may refuse to make an order of forfeiture if not satisfied on a balance of probabilities that the property is not terrorist-related property. Alternatively, if the judge is satisfied that the respondent has an interest in the property and has exercised reasonable care to ensure that the property would not be used to facilitate or carry out a terrorist act, and is not a member of a terrorist entity, the judge shall order that the interest is not affected by the forfeiture and declare the nature and extent of that interest (s.26 TSOFA).

200. A court may void transfers made to a third party after restraint was ordered unless the transfer was to a bona fide purchaser for value (s.29 TSOFA). However, the TSOFA does not contain a provision similar to section 12(7) of the CDSA which would void gifts for a six year period prior to application for confiscation.

Monitoring and sanctions

201. MAS carries out regular inspections on financial institution to ensure that they screen accounts against the UN lists (made pursuant to S/RES/1267(1999)) and comply with the relevant legislation, regulations and Notices on Prevention of Money Laundering and Countering the Financing of Terrorism. A financial institution which fails to comply with any directions issued pursuant to section 27A and B of the MAS Act – including the MAS (ATM) Regs – shall be guilty of an offence and liable on conviction, inter alia, to a fine not exceeding SGD 1 million. Additionally, financial institutions are subject to a range of civil, administrative or criminal sanctions for failure to comply with the relevant legislation, regulations and Notices (see sections 2.2 and 3.10 of this report for the full description).

Additional elements

202. Singapore has implemented some of the measures set out in the FATF Best Practice Paper for Special Recommendation SR.III. For example, unlike under the CDSA, freezing under the TSOFA can occur without prior notice to the parties whose funds or other assets are frozen and without any criminal charges being brought. The law also indemnifies persons acting in good faith when disclosing information about acts of FT to relevant authorities. Yet, the "tipping-off" provisions – adopted from CDSA – are not wholly protective of any action taken during the process of reporting suspected criminal activity to the authorities.

Recommendation 32 (Terrorist financing freezing data)

Statistics and effectiveness

203. Singapore authorities have indicated that they have not frozen any funds pursuant to designations made under S/RES/1267(1999). The following data have been provided to indicate seizures made under Singapore law enforcement mechanisms relating to the freezing, seizing and confiscation of terrorist-related funds, as requested by other countries who have made designations pursuant to S/RES/1373:

Statistics on Financing of Terrorism Investigations

	2004	2005	2006	2007 (as at 14 Nov.)
Total Nbr of Cases in which Assets are Seized	6	1	4	1
Number of Accounts in which freezing order is effected:	6	5	11	2
Total Amount of Assets Seized pursuant to FT	SGD 13 549	SGD 17 883	SGD 21 859	GBP 209/SGD 4 467
Total Amount of Assets Confiscated or Forfeited pursuant to FT	-	-	-	

2.4.2 Recommendations and Comments

204. Singapore should enact a legally-based mechanism to designate persons and organizations in the context of S/RES/1373(2001). Although procedures exist by which this can be accomplished, an exact procedure compliant with Special Recommendation III, by which Singapore will review

designations by other countries for possible designation by Singapore, should be adopted by the MHA. As the procedure currently stands, there are no articulated standards by which any decision to designate or not designate may be judged.

205. The dissemination of designated entity information pursuant to S/RES/1267 currently in place through MAS to regulated entities is adequate. A particularised delisting procedure should be implemented, as well, to specify Singapore's perceived international obligations to submit any proposed release of funds to the UN 1267 Committee for approval should be adopted.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**LC**	• Although Singapore relies on its well-honed procedures of advising its ministries and regulatory bodies of MHA's decisions to give effect to the actions initiated under the freezing mechanisms of other jurisdictions, or to designate persons in the context of S/RES/1373(2001), there is not a particularized legal framework for doing so. There is no formal delisting procedure in place. • Provisions for obtaining access to frozen funds to pay basic expenses should be made specifically subject to the requirement of obtaining approval of the 1267 Committee for funds or other assets frozen as a result of S/RES/1267(1999). As Singapore has never utilized the TSOFA procedure for freezing, restraining, or forfeiting terrorist-related property, the efficiency and speed of this procedure has not been tested.

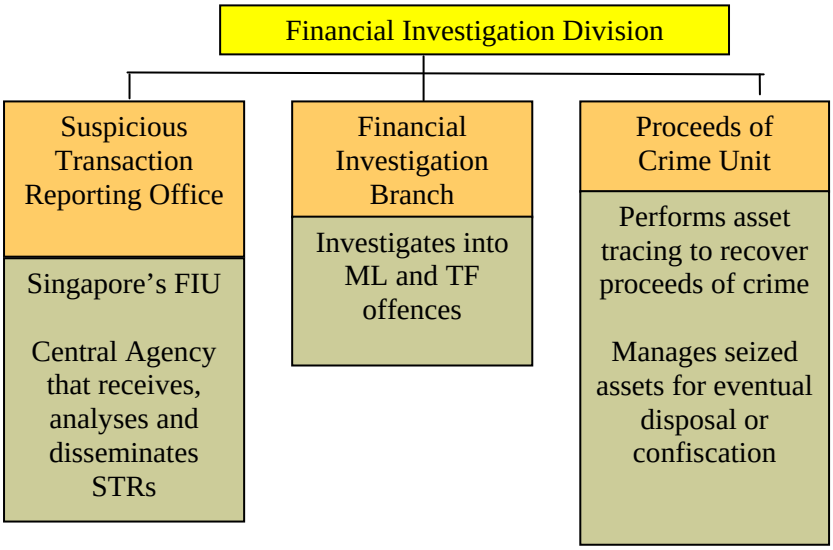
Authorities

2.5 The Financial Intelligence Unit and its Functions (R.26)

2.5.1 Description and Analysis

Functions and responsibilities of the FIU

206. The Suspicious Transaction Reporting Office (STRO) is Singapore's designated FIU. The government of Singapore approved its formation in 1999, and the STRO was established formally on 10 January 2000 as an enforcement-style FIU under the Financial Investigation Division (FID) of the CAD in the Singapore Police Force. The STRO was not established under a specific legislation but under a Ministerial direction issued as a result of a Cabinet decision STRO officers (as Commercial Affairs Officers) are deemed to be enforcement officers and are given police powers under section 64 of the Police Force Act. Nonetheless, the role of the officers of STRO, including its ability to receive, analyse and disseminate STRs, are legislatively provided for in the November 2007 amendments to the CDSA. The following chart illustrates STRO's position within FID, in relation to other relevant units.



207. STRO, as part of the FID, is the national specialist unit established to, amongst other things, to detect and prevent ML and TF activities through the receipt, analysis, and dissemination of STRs. Currently, STRO uses the provisions of section 39 of the CDSA to receive information. This legislation sets out the obligation of any person in Singapore to disclose knowledge or suspicion of property being proceeds or being used, or intended to be used, for drug trafficking or serious crime. Amendments to the CDSA effective 1 November 2007 designated the Suspicious Transaction Officer as the officer responsible for receiving the disclosures. (Previously, an 'authorised officer', which includes a Suspicious Transaction Officer, was so designated.) The STRO uses its inherent 'police powers and procedures' to analyse and disseminate STR and other relevant information. The November 2007 CDSA amendments also made the STRO the agency responsible for the receiving of information relating to the cross border transportation of currency and bearer negotiable instruments.

Publications and guidance

208. Industry-specific AML/CFT guidance notes concerning reporting obligations are issued by the respective regulators or competent authorities who are in the best position to understand the risks involved in their respective industry. The regulators, when sending out guidance notes on STR reporting to their respective industry, frequently work in partnership with STRO to include indicators on the type of suspicious transactions to report, the relevant STR reporting forms to use, as well as directions to send the STR to STRO. STRO's specific input into the development of such guidance also includes the manner of reporting STRs, the type of information that should be captured, the design of the specifications of reporting forms, and the procedures that should be followed when reporting STRs. STRO reports that these efforts have helped to enhance the quality of the STRs received by it over the years.

209. In 2006, STRO developed and implemented a STR On-Line Lodging System (STROLLS) for STR reporters. STROLLS allows STRs to be lodged conveniently and swiftly through the internet. STRO conducted numerous training sessions to the different industry sectors on the use of STROLLS in lodging STR. During these sessions, STRO shared with reporting institutions new typologies, trends and indicators, and addressed industry concerns and queries. STRO also conducted 2 major outreach sessions to over 50 financial institutions during the roll-out of STROLLS in September 2006 and March 2007. Additionally, STRO participated in a public seminar co-organised with the Money Changers Association of Singapore in February 2007. The event was attended by over 150 participants where STRO shared with the participants the importance of reporting STRs, customer due diligence as well as indicators and trends common to the money changing industry.

210. STRO provides general guidance on STR reporting on its website and through its various publications such as in the STRO/CAD Annual Report and Reports from STRO which is a regular publication that includes the latest ML/TF trends, feedback on typologies, indicators of suspicious transactions and statistics. STRO has also issued 2 editions of a Handbook on Singapore's AML/CFT regime, the latest edition being published in June 2005. A 3rd edition to appraise the reporting entities is being developed. Both the Reports from STRO and the Handbook are regularly given to STRO's strategic partners, such as the various financial institutions and other reporting entities, and are also available for download at STRO's website. Additional information on STRO's activities is published on the STRO/CAD website and in the CAD Annual Report, including a description of STRO initiatives and crime trends that are observed by STRO. In addition, subscribers to STROLLS, the online STR reporting platform, are able to access additional and up-to-date information. The information on the STROLLS bulletin pages include, amongst other things, legislation updates and indicators of a suspicious transaction.

Access to information

211. Being part of SPF, STRO has direct on-line and instantaneous access to all enforcement information including criminal records maintained by SPF via the SPF-wide computerised investigation system known as CRIMES II which contains information from all enforcement actions conducted by the SPF. The information includes: the identities of suspects, accused persons, witnesses and complainants; offences investigated, charged and convicted; sentencing details for convicted cases; the contact information of the investigating units; brief facts of the investigation; and records of supporting documents relating to the investigation. CRIMES II also has numerous interfaces with external databases such as Singapore's National Records Office and details on vehicle registration. STRO is also supported by the Intel and information network available to the police, which includes the CAD Intel Unit (and through them their network) as well as Interpol.

212. STRO officers have access to a wide variety of information, whether through a request for information to the agency or by the use of their coercive police powers (*e.g.* s.58 CPC), and can obtain information from financial institutions, including: financial records (from financial institutions); household particulars; past and present employment details; company details including details on directorship, shareholdings; family (*e.g.* births and deaths) records; bankruptcy records; travel records; marriage records; details of cars, properties, shares and securities owned by subjects; data and information on terrorists and organised crime syndicates; as well as relevant information from various government agencies. STRO officers also have access to commercially available databases and other open sources of information to facilitate the analysis and investigation of STRs.

213. STRO officers (as Commercial Affairs Officers) are deemed to be enforcement officers and are given police powers under section 64 of the Police Force Act to perform investigations. Using the police powers granted to them under section 58 of the CPC, STRO officers are able to compel reporting parties to provide additional documentation, including financial information kept by financial institutions, needed to assist it in the analysis of STRs. STRO officers may apply to court for an order to be made to compel the production of additional documentation from public bodies (*i.e.* government ministries) needed to assist in their analysis and/or investigation of financial transactions relating to drug trafficking or criminal conduct (s.40 CDSA to which s.30 is subject). However, applications for the production of documents that are in the possession of financial institutions must be made by the Attorney-General through the High Court (s.31(1) CDSA). Similar provisions in the TSOFA (section 11) allow STRO officers to seek additional information with regard to offences relating to terrorism financing.

214. The powers that STRO officers can exercise pursuant to the CDSA, TSOFA and CPC can also be used on natural or legal persons in Singapore. Overall, STRO states that the high level of cooperation between it and the reporting entities (particularly the financial institutions) is such that requests for further information are frequently provided in a timely manner: within a day for urgent cases and around two weeks for routine cases.

Analysis and dissemination of information

215. As part of their analysis of STRs, the STRO supervisors conduct a preliminary analysis to filter out or tag STRs for deeper analysis. These tagged STRs are then disseminated to CPIB and CNB for screening and/or information and/or to remove/reduce conflicts. During the de-conflicting process, STRO disseminates the information to CNB and/or CPIB to inform them of STRO's intention to conduct investigations into the STR for the purpose of establishing a money laundering offence. This dissemination is necessary as there may be the possibility that the person(s) featured in the STR are already part of an on-going or previous investigation by CNB or CPIB.

216. During this process, CNB and CPIB search their own respective internal databases and inform STRO if there is any on-going or previous investigation on the suspect(s), and any other intelligence information, previous or ongoing investigations that they might have on the entity. This process ensures that STRO does not duplicate the efforts of CNB or CPIB, and allows the agencies to coordinate its investigative efforts if necessary. Nonetheless, this does not in any way affect STRO's discretion to carry out its own investigations or additional dissemination if it feels that it is necessary.

217. STRO, as police officers, may exercise police powers in various situations during the course of investigating an STR. These powers are exercised in order to develop the STR and to identify the possible commission of a money laundering offence or other offences. (It should be noted that the Singapore authorities refer to the statistics where police powers are invoked as "money laundering investigations"; however, the team did not consider these as ML investigations *per se*, rather they are STR investigations, and the police powers were often invoked for and later used to pursue predicate offences.)

218. In certain cases, STRO may decide that it is appropriate or expedient to follow through the entire investigation up to the prosecution stage. In such cases, STRO will invoke its full range of investigative powers (including powers of interview, seizure, confiscation and arrest) under the CPC, CDSA and TSOFA to gather evidence towards the prosecution on the accused for the offences.

219. STRO may also be requested to support an ongoing predicate investigation by the relevant enforcement unit in the police, whether through STRO's links with the Egmont Network or to conduct fund tracing, as well as consider if there is any money laundering offence being committed. The table below shows the number of domestic request for assistance STRO receive for such purposes.

Domestic Request for Assistance

	2004	2005	2006	2007 (14 Nov)
Domestic Request for Assistance Received by STRO	7	2	6	13
Responses to Domestic Request for Assistance	7	2	6	13

220. If STRO develops positive intelligence as a result of the STR investigation, it may disseminate a more formal package to investigative agencies for further investigation. STRO uses its defined policing functions, under the Police Force Act and CDSA, to disseminate information and to refer matters to other agencies in Singapore. It also has, with conditions, an authority under section 41 of the CDSA to communicate information to a foreign authority. STRO has a standard operating procedure in which all disseminations of information, whether to local agencies or foreign FIUs, must be endorsed by Head of STRO or (in his absence) the Assistant Director of FID. The following chart shows the number of STRs received, tagged, STR investigations where police powers were used, and referrals forwarded to investigative agencies from 2004 to November 2007.

Number of STRs received analysed, and disseminated

	2004	2005	2006	2007 (as at 14 Nov 2007)
Number of STRs Received by STRO	1 784	2 076	3 290	6 382
STRs tagged by STRO and sent to law enforcement agencies (CNB and CPIB) for de-conflicting	695	683	1 087	1 500
STRs where STRO used police powers were invoked to gather more information[18]	442	614	963	1 442
STRs referred by STRO to investigative agencies for comprehensive investigation	106	389	549	593

221. The number of STRs received by STRO has been increasingly steadily and by over 1500% since 2000 (431 STRs). The number and quality of STRs is expected to continue to increase as STRO continues to enhance its engagement with the various reporting entities coupled with the maturity of the sectors.

222. If a ML/FT offence is detected or suspected, STRO conducts its own analysis or inquiries, and then refers the STR information (including the financial information) to the FIB for further investigation. Statistics indicate that 4 STRs have resulted in ML prosecutions and convictions since 2000. If a predicate offence is suspected or detected instead, STRO disseminates the information to other divisions in CAD or to the other investigative agencies if they are not within CAD's purview (*e.g.* to other divisions/departments within the SPF or other regulatory and/or law enforcement agencies in Singapore).

Type of predicate offence cases forwarded by STRO	2004	2005	2006	2007 (as at 14 Nov)
Corruption related	3	12	1	9
Counterfeit/Stolen Currency/ Travellers' cheques / Money transfer instruments	1	2	4	7
Drugs related	0	0	2	2
Fraud committed by corporate management / lawyers	9	7	11	6
Fraud committed by other individuals	20	6	8	55
Fraudulent banking instruments/ investment scams	5	13	18	32
Gambling related activities	11	20	54	46
Immigration offence	0	0	1	0
Money mules	0	19	57	25
Advance Fee Fraud	1	2	11	11
Advance Fee Fraud (Impersonation)	0	1	3	1
Sale of controlled items	0	0	7	6
Type of predicate offence cases forwarded by STRO	**2004**	**2005**	**2006**	**2007 (as at 14 Nov)**
Security market misconduct	5	16	11	12
Technology crime related	8	0	0	0
Terrorism Financing	0	8	11	18
Unlicensed money lending activities	43	281	343	357
Unlicensed money-changing/remittance operations	0	2	7	6
Total	**106**	**389**	**549**	**593**

[18] It should be noted that Singapore considers these to be "money laundering investigations", whereas the assessment team considered them to be STR investigations and not ML investigations *per se*.

223. Analysis of the statistics provided for STRs reflects an overall tendency within the SPF to focus on the predicate offence (an issue which is elaborated further in sections 2.1 and 2.6 of this report) and appears to support that the STRO is focused on predicate offences, rather than money laundering cases. However it should be noted that many of the predicate offences (referred to in the table above) have a money laundering 'flavour' and could arguably be considered the basis of later money laundering investigations conducted by various areas of the SPF.

224. For domestic predicate offences, STRO's strategy is to analyse the STRs to establish the commission of any predicate offence and when such offences are detected, the STRs are then referred to the relevant CAD investigative units or other investigative agencies to consider if there are sufficient grounds to launch a full-scale investigation on these predicate offences. Once a full-scale investigation is launched, the investigative agencies may then work jointly with PCU and FIB to commence any money laundering investigations arising from the predicate offences.

225. In over 200 cases where the STRs involve possible proceeds generated by foreign predicate offence, STRO has approached its foreign counterparts to establish if the foreign predicate offence would result in a money laundering offence in Singapore. If a nexus with the foreign predicate offence is ascertained, the money laundering investigation is referred to FIB or PCU for further investigation. STRO has made 109 referrals to FIB/PCU between 2004 to 14 November 2007 in relation to money laundering involving foreign proceeds of crime. These have resulted in 15 cases of money laundering investigations relating to a foreign predicate offence and resulted in approximately SGD 109 million of proceeds of crime seized.

Breakdown of referred STRs involving Foreign Predicate Offences

	2004	2005	2006	2007 (as at 14 Nov.)
No. of STRs involving foreign predicate offences forwarded to FIB/PCU	1	19	59	30

226. Physical security of information is ensured by STRO's location within SPF premises and with STRO's officers allocated their own secure office and storage facilities. The office rooms and metal cabinets are locked and accessible only by the officers themselves. IT information security for STRO includes a secure portal for STRs to be lodged electronically via the internet in encrypted form. The STRO database (which includes all STR information) is restricted to STRO officers and cannot be accessed by other officers in the SPF without STRO's consent. The system is password protected and an audit trail is available if required. Apart from STRO officers, the only other personnel authorised to access STR information are the Assistant Director FID (to whom Head STRO reports directly to), and the Senior Deputy Director of CAD, who is in charge of all operational matters in CAD. CAD officers not working within STRO are not given access to the STRO database, but STRO is automatically alerted by the system if an entity that is featured in an STR is also featured in an investigation. STRO may then proactively seek information from the investigating officer and/or disseminate STR information to the officer.

227. Additionally, information is disclosed within STRO only on a "need to know" basis. In cases where the information is very sensitive, STRO officers can choose to upgrade its security classification requiring further authentication before any access is granted. However, if the computer system shows a connection between STRs that are being handled by different STRO officers, these STRO officers may discuss their STRs together with their supervisors and/or the Head of STRO.

Operational independence and autonomy

228. The assessment team was informed that although the STRO is a branch within the FID (which is a division of CAD), it has a dedicated, full-time staff, none of whom are assigned to perform other non-FIU related police duties, and that there is sufficient operational independence and autonomy to ensure

that it is free from undue influence or interference. Further it was indicated that STRO is funded from the CAD budget and is able to leverage on the CAD budget, and even the overall SPF budget in certain areas. STRO is of the view that this arrangement works to its advantage. It may, for example, tap into funding that is greater than the usual funding of a comparable unit of similar size. This was illustrated when STRO embarked on the STROLLS project. STRO was also able to access SPF funds for the development of WINGS, a specialised and customised web-based analytical tool for analysing and prioritising STRs. The total cost of these two computerisation projects is approximately USD 1 million.

229. However, there are still concerns about the STRO being sufficiently operationally independent with sufficient autonomy to be free from undue influence or interference. In Singapore's case, unlike other jurisdictions that have police FIUs, there does not appear to be any formal administrative or legislative provision regarding the setting up the STRO, defining its role or setting out the quarantining of resources. The authorities indicated that the STRO was set up and merged into the SPF as the consequence of a Cabinet decision. Cabinet documentation relating to this decision is classified as secret and was not provided to the team. Another point is that currently the head of CAD, not the head of the STRO, signs the MOUs between STRO and foreign FIUs. Currently the STRO is strongly supported by the government and the authorities firmly believe that the support of the Government is unlikely to change. However, although STRO is currently the subject of positive political will, with increasing resources and quarantining of resources, there are future concerns if the political commitment changes.

Egmont Group

230. STRO was officially accepted into the Egmont Group of FIUs in June 2002. Since then, it has actively and consistently attended Egmont Plenaries and the Meetings of the Heads of FIU each year. In 2005, STRO became a member of the Egmont Group's Fund Administration Sub-Committee. STRO has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange. The mechanisms for STRO's exchange of information with its foreign counterparts is discussed in detail in section 6.5 of this report.

Recommendation 30 (Resources of the FIU)

Funding

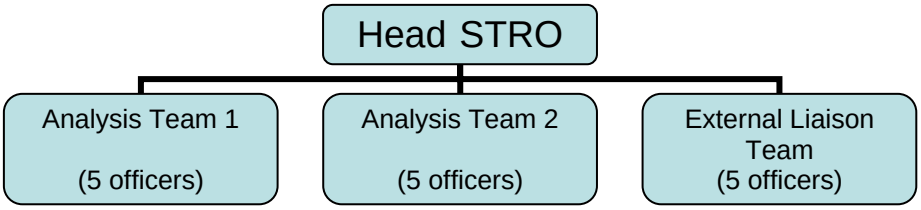
231. Overall, the STRO is well funded, structured and resourced. The funding for STRO is part of the CAD's Operational Budget in terms of manpower costs as well as in the planning and implementation of various AML/CFT projects. There has not been an occasion where any of STRO's AML/CFT projects could not be implemented as a result of inadequate funding. It has also been one of the fastest growing units within CAD. STRO expects a further increase in budget and intends to recruit more officers in fiscal year (FY) 2007 and FY 2008 as part of the management's strategic plans to enable STRO to take on additional challenges in relation to the implementation of the new declaration system and to manage the AML/CFT risk arising from the setup of the 2 casinos in 2009. The table below contains the estimated STRO's budget/expenditure including the cost of manpower, local and overseas training, publications, outreach, staff welfare, utilities and general supplies, use of office space, as well as the development and maintenance of IT projects such as STROLLS and WINGS.

	CAD's Budget	Estimated STRO's Budget/Expenditure
Financial Year 2004	SGD 11.9 million	SGD 2.0 million
Financial Year 2005	SGD 12.9 million	SGD 2.1 million
Financial Year 2006	SGD 13.2 million	SGD 2.1 million
Financial Year 2007	SGD 13.3 million	SGD 3.8 million

Note: Financial Year starts from 1 April of the year to 30 March of the next year.

FIU structure and human resources

232. The Head of STRO is under the supervision of the Assistant Director FID who reports to the Deputy Director/Director of CAD. STRO officers are mainly investigating officers who have tertiary and professional qualifications in accountancy, business and law. They are divided into teams of four, each led by an experienced team leader. Two teams are responsible for performing analysis and one is responsible for external liaisons. The External Liaison Team's complement of five officers includes a team leader and two Assistant Investigation Officers (AIOs) with diplomas in business and legal studies. The AIOs also have previous working experience in law firms or insurance companies and thus possess a good working knowledge of these sectors which has imbued them with a sound and practical outlook in their work. The below diagram illustrates STRO's internal structure.



233. The two Analysis Teams are responsible for: (1) reviewing, analysing and inquiring into STRs for the detection of ML, FT and other predicate offences; (2) disseminating STRs and liaising with other relevant investigation units on investigations relating to STR information; and (3) researching the latest ML trends and indicators for suspicious transaction reporting. The Analyst teams work closely with the External Liaison team to identify trends and threats for feedback to the reporting entities, with a view to enhancing the quantity and quality of STRs lodged. In addition, the Analyst teams conduct periodic reviews of the STRs analysed and perform profiling of STRs to assess the AML/CFT situation in Singapore.

234. The External Liaison team develops and implements STRO's efforts to raise awareness on AML/CFT issues, liaises with reporting entities on issues relating to the lodging of STRs and provides them with operational assistance. These activities include planning and conducting outreach programs to financial institutions, DNFBPs and the general public, designing STRO's policies on outreach programs, distribution of STRO's AML/CFT publications and publicity materials, and obtaining and analysing feedback. The External Liaison Team is also responsible for negotiating MOU with other FIUs, and represents STRO in dealing with local and foreign counterparts to facilitate STRO's involvement in the development of AML/CFT issues. This includes reviewing policy considerations relevant to STRO's operations and functions.

235. STRO's manpower has increased from an initial five in 2000, to nine in 2003, to the current 16 officers in 2005. There is currently a proposal to further increase STRO's staff, before the two Integrated Resorts (with casinos) become operational in 2009 for the purpose of liaising with the two casinos and analysing casino-related STRs and cash transaction reports. Serious consideration is also being given to increasing manpower for the processing and analysis of cross-border currency and negotiable bearer instruments declaration forms for the implementation of the new declaration system.

Technical resources

236. STRO has access to a wide array of tools to assist it in the receipt, analysis, dissemination and management of STRs submitted to it. Apart from the traditional receipt of STRs via post or courier, STRO has since developed an online STR reporting system, STROLLS, which is integrated with an SGD 20 million advanced case management system (CRIMES-II) which is used to manage the processing and analysis of the STRs. STROLS and CRIMES-II are both described above in more detail. For more in-depth analysis, STRO also uses i2, a popular and powerful analytical tool to assist in the analysis and investigations of STRs. To further enhance its operational capability and provide a

greater range of analytical tools to the STRO investigating officers, STRO is developing a new IT system known as WINGS (Web-based Intelligence Analytical and Graphical visualisation System) that costs SGD 1.5million.

Professional standards, skills and confidentiality of staff

237. STRO officers are selected based on merit having regard to tertiary educational qualifications and experience, and taking into account the mission of the department and STRO. They are regularly appraised on a half-yearly basis on their competencies and contribution to STRO's work. Integrity ranks as one of the key considerations in the recruitment and positing of officers to STRO. STRO's Team Leaders and the majority of the Investigation Officers also possess extensive investigation experience, including those relating to ML/FT. This allows them to guide their teams in identifying the evidential requirements of an investigation and prosecution, resulting in the timely generation and dissemination of high quality financial intelligence data.

238. All STRO officers are screened and security cleared by the Internal Security Department upon joining. The Head of STRO and other STRO officers tasked with analysing STRs related to terrorism financing are also required to pass a higher level of security clearance before performing such work.

239. STRO officers (and for that matter all authorised officers) are obligated not to disclose any information (including STR information) obtained in the course of their duties, except for designated purposes (s.56(1) CDSA). A breach of this provision is punishable on conviction to a fine not exceeding SGD 2 000 and/or imprisonment for a term not exceeding 12 months. Moreover, as public servants, STRO officers are bound by the Official Secrets Act (Cap 213) (OSA) which prohibits the communication of any information that is obtained by a person by virtue of his/her service with the government in a manner which is contradictory to lawful directions issued with regard the information or which is without reasonable care to the safety of the information (s.5 OSA).

Training

240. Training for new STRO officers includes a series of lectures on relevant laws relating to ML, FT and criminal procedure. STRO analysts participate in monthly 4-hourly in-house training sessions, called In-service Training, conducted at the FID division level. During such sessions, in-house and/or external speakers are invited to present topics on specialised crime investigation areas; with a focus on AML/CFT. This allows FIU analysts (STRO), proceeds of crime specialists (PCU) and financial investigators (FIB) to exchange information and concepts in their area of expertise in AML/CFT. Each STRO officer must receive at least 48 hours of AML/CFT related training every year. STRO also sends officers to AML/CFT courses both locally and overseas, including courses organised by overseas FIUs and enforcement agencies, and local agencies like CPIB and CNB.

Recommendation 32 (FIU):

Statistics and effectiveness

241. STRO maintains statistics on the number of STRs received, analysed and disseminated (see the above chart), including a breakdown of the type of financial institution, DNFBP, or other business or person making the STR (see statistics in section 3.6 of this report). STRO is also developing the WINGS systems which will include a comprehensive module for the accurate and up-to-date retrieval of a variety of statistics.

Additional Elements

242. Singapore's also maintains comprehensive statistics on STRs resulting in the prosecution or conviction for ML/FT, as indicated in the following chart.

Number of STRs received resulting in prosecution and conviction

	2004	2005	2006	2007 (14 November)
STRs Resulting in (ML) Prosecution	2	1	-	1
STRs Resulting in (ML) Conviction	1	1	1	1
ML investigations (full scale) as a result of STRs	3	2	3	14
Funds Seized / Frozen relating to ML / TF pursuant to STR Information	SGD 5 824 396 USD 360 038 AUD 130 000	USD 1 500 303	SGD 7 938 155 USD 4 229 694	SGD 8 815 369 USD 70 000 MYR 7 000 EUR 46 538 535

2.5.2 Recommendations and Comments

243. STRO's outputs do not appear to be leading to the detection, investigation or prosecution of money laundering, particularly in relation to proceeds generated by foreign predicate offences. STRO's analysis appears to have a higher concentration on predicate offences, rather than money laundering offences. While STRO claims its main focus is in the detection of ML and FT offences, the STRs analysed are frequently in relation to predicate offences and are being referred, when appropriate, for the investigation of predicate offences. Statistics indicate that of the total STRs, (including 200 possible foreign predicate identified – 109 referred) four STRs have resulted in ML prosecutions and convictions. STRO has been successful at identifying specific (usually domestic) predicate offences through its analysis. However, evidence of foreign predicate offences is more likely to exist outside of Singapore; therefore, overly focusing on the detection and identification of the predicate offence results in an approach that is unlikely to capture money laundering related to the proceeds generated by foreign predicate offences. Given the known AML/CFT risks in the region, and the potential attractiveness of Singapore as a large, stable and sophisticated financial centre through which to launder money, STRO should ensure that it continues to stay focused on the identification of ML offences, particularly ML involving the proceeds of foreign predicate offences. Once STRO has refocused itself in this way, it should give consideration as to whether it has sufficient resources to manage this workload.

244. The Singapore authorities should strengthen the operational independence of this FIU to ensure that the current political commitment to the STRO's operations does not change with future governments. In addition, the STRO should more proactively target the detection of money laundering cases, particularly those involving proceeds generated by foreign predicates, rather than focusing on identifying predicate offences. Singapore should also take steps to ensure that the process of the police 'de-conflicting' STRs before they are analysed by the STRO does not undermine its independence as an FIU (*i.e.* by acting as a filter of the FIU's activities).

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**LC**	• STRO's analysis is overly focused on detecting and identifying predicate offences, and is not adequately focused on detecting and identifying money laundering cases. • Minor concerns about the operational independence of the STRO.

2.6 Law Enforcement, Prosecution and other Competent Authorities – the Framework for the Investigation and Prosecution of Offences, and for Confiscation and Freezing (R.27 and 28)

2.6.1 Description and Analysis

Recommendation 27 (Designated law enforcement authorities)

245. ***Financial Investigation Branch (FIB):*** The FIB (located within the Financial Investigation Division of CAD) is the lead enforcement agency in ML/FT investigations within the SPF. The key role of FIB is to investigate all money laundering investigations and provide cross-jurisdiction assistance relating to money laundering for matters under the purview of the SPF. The FIB is also the lead unit in handling novel areas of ML investigation, at least until such time when an appropriate investigative unit can take over, with a view to ensuring that all ML investigations are handled in an expedient manner. Additionally, the FIB is the unit responsible for investigating FT offences, including tracing the assets of the suspected terrorists to ensure that the assets are frozen in a timely manner. The work of the FIB is complemented by its sister unit in the SPF, the Proceeds of Crime Unit (PCU) (see description below under the heading of "Additional elements").

246. ***Financial Investigating Team (FIT) of the Central Narcotics Bureau (CNB):*** Under the CDSA, the CNB is authorised to investigate ML offences, and has established its own specialist investigative unit (the FIT) to investigate ML offences that are related to drug trafficking. The FIT does augmented financial bank / screening on behalf of other operational CNB divisions for drug predicate offences, such as trafficking and importation. In cases where the money laundering involves an international element, the CNB will work with the FIB to ensure the expeditious resolution of the matter. It also focuses on the seizure, freezing and confiscation of proceeds of crime from scheduled CDSA drug offences.

247. ***Financial Intelligence Branch of the Corrupt Practices Investigation Bureau (CPIB):*** The CPIB is also authorised, pursuant to the CDSA, to investigate ML offences, and has established its own specialist investigative unit to investigate ML offences that are related to corrupt practices – the Financial Intelligence Branch which is located within the CPIB's intelligence unit. The key roles of this Branch are to look at all STRs that are referred by CAD, investigate ML offences that are related to corrupt activities and provide cross-jurisdiction assistance relating to corruption investigations. The Financial Intelligence Branch reports directly to the Head of Intelligence and is headed by the Head of Strategic Intelligence. The unit works closely with the local FIB or their foreign counterparts if the case relates to the laundering of corrupt proceeds, with a view to ensuring that the investigations are conducted expeditiously. CPIB also investigates all corruption offences, and enforces the Prevention of Corruption Act (PCA) and the CDSA in relation to the confiscation of benefits derived from corruption and other serious crime.

Postponement of Arrest and/or Seizure of Monies

248. There is no provision in Singapore law that would prevent the competent authorities investigating ML cases from postponing or waiving the arrest of suspected persons and/or seizure of the money for the purpose of identifying persons involved in money laundering or terrorism financing activities or for evidence gathering. Consequently, it is implicitly allowed. In CAD's context, the arrest of a suspect is usually made at the later stage of the investigation in order to facilitate evidence gathering, for the purpose of identifying other suspects, and for asset tracing and recovery. However, these prerogatives are exercised judiciously and require the approval of CAD senior management to ensure that such measures are appropriately supervised and not abused.

Additional elements

Special investigative techniques

249. Singapore's law does not contain any restrictions on the ability of law enforcement agencies to carry out co-ordinated investigations (with domestic or foreign counterparts) using special investigative techniques (including controlled deliveries, continued surveillance and undercover operations), to the extent appropriate in each case and subject to necessity. For example, the CDSA authorises the police to use surveillance techniques in the context of investigating ML. Specifically, an officer may consent to allowing a person to perform certain acts of ML for the purpose of gathering evidence (s.44(3)(a)(i) CDSA). In the case of certain investigative techniques that are intrusive and potentially violate the privacy of individuals, the law enforcement agency must first seek authorisation from the Public Prosecutor who will independently evaluate the necessity for the use of such techniques. The Singaporean authorities state that special investigate techniques are used whenever necessary and beneficial to a ML/FT investigation.

Groups specialising in the investigations of proceeds of crime

250. ***Proceeds of Crime Unit (PCU):*** The PCU is a specialised unit within the FID that is focused on identifying and retrieving the proceeds of crime. It role is to assist investigative/enforcement units within the SPF in the tracing, recovery and management of proceeds of crime until their eventual disposal by a court of law. Where applicable, the work of the PCU is complemented and supported by the FIB. In the course tracing funds, the PCU is also empowered to follow up on any ML activities that it may have uncovered. The officers from the PCU are also trained to handle and manage seized assets (*e.g.* gold bars, motor vehicles, condominiums and pleasure craft) so as to preserve their value for eventual disposal or confiscation to the state. Between 2000 and 2006, the PCU/FID managed to recover in excess of SGD 110 million in proceeds of crime. Additionally, the PCU also involves itself in the investigation into offences under the Money-Changing and Remittance Businesses Act and is thus familiar with typologies associated with the alternative remittance businesses.

Review of ML/FT methods, techniques and trends

251. The FIB's two financial investigative teams are tasked with reviewing ML/FT methods, techniques and trends in Singapore, including asset recovery and management techniques, in accordance with their particular specialities. Such periodic review has led the teams to produce various research products, such as Frauds Committed by Bank Officers (which profiles various cases of frauds committed by bank officers in their official capacity, and offers recommendations on how the banks may prevent such frauds) and the Joint Casino Paper on Pathological Gambling and Crime (which examines into the nexus between a pathological gambler and the propensity to commit crime). FIB has also performed detailed financial profiling into the transaction activities of known Jemaah Islamiyah (JI)

252. The core function of the Police Intelligence Department (PID) of the SPF is to provide timely and accurate intelligence, and to assist the operational units in making informed decisions. The PID's Crime Pattern Analysis Branch (CPAB) is in charge of analysing crime trends, patterns and the modus operandi employed by the perpetuators. The CPAB disseminates crime alerts and has produced several research papers into various offences, some of which are predicate offences listed under the CDSA (*e.g.* unlicensed money lending). Several of these research papers are circulated to the relevant departments (*e.g.* STRO) to complement their analysis of STRs. PID has also created a Counter-terrorism portal that is available through the SPF Intranet and can be accessed by the various law enforcement agencies. Through this portal, PID provides timely updates on the significant threats and incidents internationally; profiling of key terrorist groups; learning points from significant terrorist attacks; and the methods/techniques utilised by the terrorist groups to achieve their ideology and purpose. Additionally, one of the roles of the STRO's External Liaison Team is to identify, initiate and research current AML/CFT trends and threats in Singapore (as described in section 2.5 of this report).

Recommendation 28 (Investigative powers)

253. Officers of the FIB, PCU and the SPF are empowered under the CPC, CDSA and TSOFA to exercise a variety of investigative powers, including the powers of seizure, confiscation and arrest. CAD officers are authorised with the same powers of investigation pursuant to section 64 of the Police Force Act (PFA). In addition to being empowered under the CPC and CDSA, officers of the CNB and the CPIB are also able to exercise their powers of investigations under the MDA and PCA respectively when the predicate ML offence is related to drug or corruption offences.

Powers of Production

254. Police officers or the court are able to compel the production of documents (including those belonging to financial institutions) or any thing that is necessary or desirable for an investigation, inquiry, trial of other proceeding. A police officer may issue a written production order (s. 58 CPC) and present it to the person who is believed to have possession or power over the document/thing. Likewise, a court may issue a summons for production. In the case of bankers' books, these powers must be exercised by a police officer who is at the rank of inspector or higher. This is a general summons provision widely used within the enforcement field. There are also specific information gathering powers under sections 30 and 31 of the CDSA. When investigating drug trafficking or criminal conduct. Officers authorised pursuant to section 30 of the CDSA may apply to the court for a production order; however, these provisions do not apply to information being sought from financial institutions. If the documents or material being sought is in the possession of a financial institution, the more cumbersome provisions under section 31 of the CDSA apply (as described in section 2.3 of this report). The assessment team was informed that section 58 of the CPC is more commonly used to obtain banking information than section 31 of the CDSA. However, it should be noted that the powers in relation to section 31 of the CDSA in no way limits the powers in section 58 of the CPC; section 31 simply provides an additional production power in relation to drug-related cases as do the Division 2 search powers in the same Act. Additionally, if a person has provided information to the Commissioner of Police (which includes a police officer) concerning terrorist-related property, the Commissioner may require that person to furnish other information or particulars (s.8 TSOFA).

Powers to search and seize

255. In the context of investigating ML, FT or a predicate offence, officers authorised pursuant to the CDSA may apply to the court for a search warrant in relation to any specified premises in cases where there are reasonable grounds to believe that the specified person (or premises) has benefited from a criminal conduct or drug trafficking activities (s.34(1) CDSA). The officer is also authorised to seize and retain any material (other than items subject to legal privilege) for the purpose of the investigation, provided that it is likely to be of substantial value (by itself or together with other material) to the investigation (s.34(5) CDSA). Police officers at the rank of sergeant or above are also authorised to search any premises if they have reasonable cause for suspecting that stolen property is contained therein, and if there are good grounds for believing that recovery of such property would be jeopardised by the delay in obtaining a search warrant (s.69(1) CPC).Law enforcement officers also have powers to restrain or seize any property that is suspected to be stolen or which is found in circumstances creating a suspicion of the commission of any offence (s.68(1) CPC). In the context of investigating drug offences, CNB officers may also exercise the powers to search and seize specified under sections 24, 25 and 26 of the MDA. Additionally, as described in detail in sections 2.3 and 2.4 of this report, there are extensive powers in the CDSA, TSOFA and MDA to seize or restrain any property that may become subject to confiscation.

Witness statements

256. Officers are generally authorised to record statements made by witnesses (s.121 CPC) or persons who are to be charged formally in court (a so-called "cautioned statement") (s.122 CPC). Additionally, officers are authorised to record statements that could be tendered with regard to any

matters relevant to the determination whether benefits have been derived by the defendant from drug trafficking or criminal conduct (s.9(1) CDSA). When investigating corruption or the laundering of related proceeds, the CPIB has a special power to make inquiries of any person who is then legally obliged to furnish information pertaining to the investigation. Any person who fails to give information or knowingly gives misleading information to any CPIB officer is guilty of an offence that is punishable by a fine not exceeding SGD 10 000 and/or imprisonment for a term not exceeding one year (s.27 PCA).

257. Generally, enforcement agencies can compel the attendance of witnesses to assist in their investigations, including those relating to ML/FT (s.120(1) CPC). This power is exercised by issuing a summons in writing to any person who is within the limits of Singapore and who may have information beneficial to the case. If someone refuses to comply with such a summons, a warrant may be issued to secure their attendance (s.120(2) CPC). In such cases, the enforcement agencies are also entitled to take up an action against the witness for non attendance in obedience to an order from a public servant (s.174 Penal Code). Such an offence is punishable by a fine and/or imprisonment.

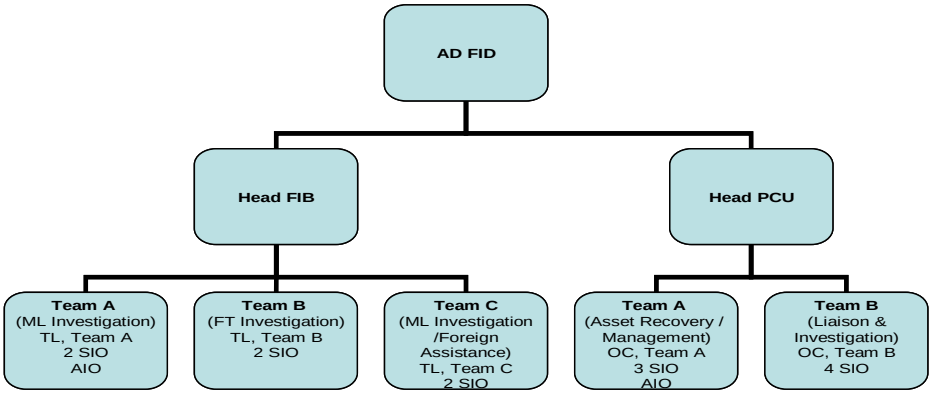
Recommendation 30 (Resources of law enforcement and prosecution authorities)

Structure and resources of law enforcement and prosecution authorities

FIB and PCU

258. The FIB (and PCU) is adequately funded by CAD/SPF's budget in terms of manpower costs as well as in the planning and implementation of various AML/CFT investigations and projects. The Singapore authorities report that funding for FIB projects has never been a problem and, in fact, the manpower for the branch was recently increased from eight to eleven. This enables the branch to handle the possible increase in workload with regard to the anticipated increase in mutual legal assistance requests.

259. The FIB consists of three teams and a total of eleven investigation officers: one Head (who is under the supervision of AD FID and who reports to the Senior Deputy Director/Director CAD), three Team Leaders, six Senior Investigation Officers and one Assistant Investigation Officer (AIO). The PCU comprises two teams and a total of eleven investigation officers: one Head, two Officers in Charge (the equivalent of a TL), seven Senior Investigation Officers and one AIO. While investigations in the FID are usually carried out under a lead investigator, the approach is also team-based and all ML/FT investigations are closely supervised by the respective TLs/OCs and their supervisors. The FIB officers are mainly Investigating Officers divided into teams of two to four persons, led by a Team Leader. They are generally assigned to the following areas of work: conducting investigations into ML/FT offences; rendering assistance to foreign authorities informally and through the mutual legal assistance framework; and investigating offences committed by employees of financial institutions in their official capacity. The Structure of FIB and PCU is appended below:



260. Both the FIB and PCU use CRIMES-II to analyse and manage their cases. They are also able to tap into the resources available generally to the SPF, including the various SPF databases. The FIB and PCU also maintain a close working relationship with STRO and could, subject to the strict internal controls, leverage on STRO's intelligence database.

261. FIB investigators generally possess university qualifications from disciplines such as finance, accountancy and economics. Several of them have professional qualifications in accountancy (Certified Public Accountant) and are pursuing certification such as a Chartered Financial Analyst. They have an average of three years investigation experience, with some officers having served in the FID for more than 10 years. They are supported by one Assistant Investigation officer with a degree in business administration. Their selection criteria are similar to those of the STRO officers and they are also subject to half-yearly competency and performance reviews with regard their work in the FIB. This includes reviewing their training needs and selecting suitable courses that are particular to the needs of the officer. Such courses are planned in addition to the regular and specialised training that is provided to FIB officers. Reward and remuneration is also similar to STRO officers.

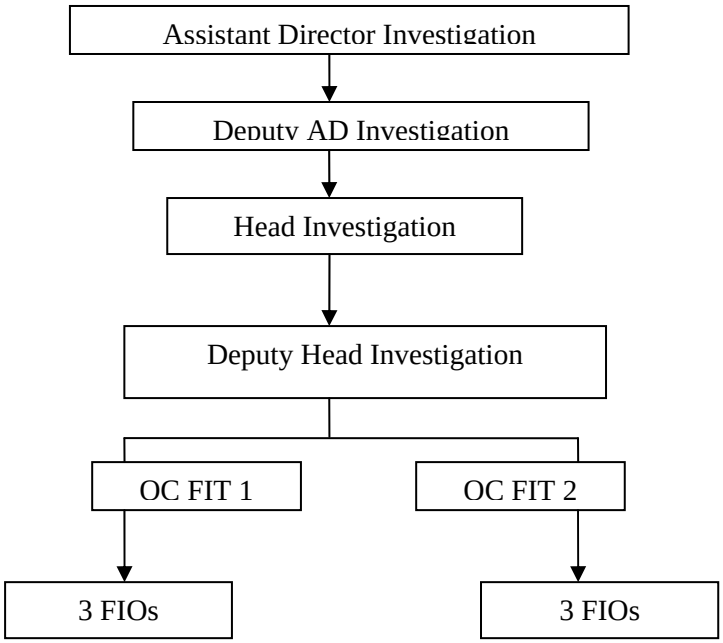
262. PCU investigators are selected from experienced police officers (and investigators) from various SPF investigation units. Most possess tertiary qualifications including Master degrees. Their work is supported by an Assistant Investigation officer with a diploma in business and who is pursing a degree in business. The eleven highly-qualified PCU investigators therefore provide a complementary role to the FIB.

263. In addition to the secrecy requirements that apply to STRO officers, FIB officers are required to be cleared at a higher security level which subjects them to a stringent security clearance, including background and integrity checks. PCU officers are subject to the same level of professional integrity and confidentiality as required of the STRO officers. Like STRO officers, both FIB and PCU officers are subject to the Code of Conduct (CAD Operation Manual, Section C4) and the confidentiality provisions of the Official Secrets Act (OSA). The authorities report that, to date, FIB and PCU officers have demonstrated a high level of integrity, maintaining a 100% complaint-free and disciplinary action-free record.

264. FIB and PCU officers obtain the same type of training that is received by STRO officers and which is described in detail in section 2.5 of this report. FIB and PCU officers have at least an average of 48 hours of AML/CFT related training every year. As well, they rely on the internal guidelines and standard operating procedures (SOPs) when conducting its investigations. These SOPs cover various different type of investigations in which the FIB and PCU officers are involved in and document important and useful administrative and investigative tips that an investigator has to look out for during the course of an investigation. A debriefing is conducted at the end of each investigation (particularly major ones). The key learning points or investigative techniques are then shared with the FID, documented and updated in the SOPs. This is usually done by the respective teams involved in the investigations.

Financial Investigating Team (FIT) of the Central Narcotics Bureau (CNB)

265. The FIT (formerly the Financial Investigation Division) consists of eight investigation officers in two teams. The two teams of investigators are led by an Officer-in-charge (OC) each and comprise three financial investigation officers (FIOs). The OCs report to Head of Investigation or, in his/her absence, the Deputy Head. The financial investigation officers are responsible for conducting ML investigations involving drug traffickers (including forfeiting their drugs and proceeds), assisting other divisions in conducting financial screening requests prior to the arrest of the drug traffickers, assisting in the screening of STRs, and rendering assistance to foreign authorities informally and through the mutual legal assistance and extradition framework. The FIT's organisation and structure are reflected in the diagram below:



266. CNB also maintains high professional standards when managing financial investigations. There are regular internal compliance checks and financial investigations are expected to be completed within the stipulated timeframe. Basic supervisor oversight and compliance checks serve as a general guide to the FIO in the course of their investigation with a view to ensuring greater transparency and safeguards the integrity of the investigation of financial process.

267. New CNB officers are required to attend intermediate and advanced CNB investigation courses within their first year in FIT to enhance their financial investigation skills and knowledge. Courses are constantly reviewed to ensure that training materials are up-to-date with current trends or situations. Officers are also sent to local and overseas courses conducted by external agencies. On-the-job training is also provided through guidance from supervisors. CNB also conducts regular in-service training for all narcotics officers (including FIT officers) to update them on the latest standard operating procedures, drug trends and related market technologies. In addition to personally attending such courses, officers also benefit from attending presentations organised by established training departments of agencies like NCID. These presentations expose FIT officers to global developments in crime and investigative techniques shared by the course attendees.

Financial Intelligence Branch of the Corrupt Practices Investigation Bureau (CPIB):

268. CPIB has a specialised Financial Investigation Branch to investigate into the laundering of corrupt/criminal proceeds under the CDSA. It is adequately structured, staffed and provided with resources to fully and effectively perform their functions.

269. CPIB officers are required to be cleared at a high level of security. The Official Secret Act also applies to all CPIB officers and it is in the bureau's code of conduct for officers that they do not discuss details of any investigation with any unauthorized persons. There are internal checks in place and it is very rare that an officer's integrity is compromised. The high standards of professional conduct required of CPIB officers is further emphasised in the Government's Instruction Manual (IM2L – Conduct and Discipline). The rules apply to every serving officer of the civil service (including all FIB, PCU, CNB and CPIB officers) and are described in detail in section 2.5 of this report.

270. CPIB shares the same training structure as the FIB within the CAD (see the detailed description above). Training its own officers is always one of the Bureau's key priorities. The CPIB has invested numerous hours in training its officers in the investigation of ML corrupt/criminal proceeds. As ML is getting more complex, the Bureau is constantly sending officers for relevant trainings both locally and overseas in order to gain more knowledge and skill.

Attorney-General's Chambers (AGC)

271. The office of the Attorney-General (AG), who is also the Public Prosecutor, is constitutionally entrenched and protected. The Attorney-General's Chambers (AGC) is the organisational extension of the AG and an independent Organ of State. It has an Autonomous Agency status, which means that it has the autonomy to determine how to utilise its allocated budget in accordance with the law and government financial practices. This institutional arrangement ensures optimal operational independence and autonomy, and freedom from undue influence or interference.

272. With 5 legal divisions, the AGC is adequately structured, funded, staffed, and provided with sufficient professional, technical and other support resources to fully and effectively perform its various AML/CFT functions. Its Legislation Division drafts the relevant primary legislation and assists in updating relevant subsidiary legislation. Legal advice to government agencies on AML/CFT matters, depending on the focus, can be provided by the Criminal Justice Division, Civil Division, International Affairs Division, and the Law Reform and Revision Division. Requests for mutual legal assistance and extradition are centrally dealt with by the Advisory Directorate of the Criminal Justice Division, which is headed by a Senior State Counsel and staffed by 7 experienced prosecutors. The Criminal Justice Division also has a dedicated Corruption and Specialist Crimes Directorate, and a Financial and Securities Offences Directorate, each headed by a Senior State Counsel and staffed with adequate number of prosecutors to deal with the more complex predicate and ML offences. Prosecutors are also responsible for applications for court orders pursuant to the CDSA, TSOFA and other written laws as and when required.

273. AGC has an organisational Code of Conduct. AGC officers are guided by the relevant Government Instruction Manual provisions concerning conduct and discipline as well as training of public servants. They are also subject to the provisions of the Official Secrets Act which prescribes high standards of confidentiality to be observed by public servants in respect of handling information obtained in the course of official duties. Prosecutors and state counsels are also expected to maintain high ethical and integrity standards consistent with the relevant provisions of the Legal Profession (Professional Conduct) Rules.

274. Both prosecutors and state counsels are provided with a structured prosecutor training course that covers AML/CFT aspects, and on-the-job training. The annual prosecutors training course must be attended by new officers and may be attended by existing officers as part of continuous professional learning. The trainers, who are the more experienced and senior prosecutors, share relevant case studies to complement the theoretical aspects. Periodically, these topics are also covered in seminars or workshops organised by the Criminal Justice Division for knowledge sharing and outreach. AGC emphasizes training to upgrade and sharpen the legal and prosecutorial expertise of its staff and has a budget to provide regular training for each staff. Courses that they attend including local or international seminars, conferences and workshops on AML/CFT organized by FATF and other agencies with an interest in AML/CFT.

Additional elements

275. In November 2006, judges were invited to a seminar on mutual legal assistance organised by AGC during which issues on ML and FT offences, and the seizure, freezing and confiscation of property were discussed.

Statistics and effectiveness

276. Initially, the number of ML investigations was relatively low, although the following statistics do show a general increase and improvement across the board. This is due to both the increase in the number of STRs leading into ML investigations as well as from predicate offence investigations. However the majority of ML investigations appear to be as a result of domestic predicate offence investigations. The following figures do not take into account the number of STR investigations which STRO conducts for the purpose of establishing a ML offence. If these were considered part of ML investigations then the figures would be more reasonable.

Statistics on Money Laundering Investigations

	2004	2005	2006	2007 (as at 14 Nov)
STRs where STRO invoked police powers to gather more information[19]	442	614	963	1 442
ML Investigations (Full Scale) as a Result of STRs	3	2	3	14
ML Investigations as a Result of Predicate Offence	7	6	26	32
Total Number of ML Investigations (Full Scale)	10	8	29	46

277. Since 2004, the number of FT investigations has been fairly steady. The following chart examines the number of STRs received by STRO that related to terrorist financing, including how many investigations resulted from those STRs. As a frame of reference, the total number of FT investigations has been included (*i.e.* including those that commenced other than through the receipt of an STR).

Statistics on Financing of Terrorism Investigations

	2004	2005	2006	2007 (as at 14 Nov)
STRs relating to Financing of Terrorism	34	49	73	313
FT related STRs concerning which STRO invoked Police Powers to gather more information	34	17	35	56
Other FT Investigations	43	33	42	39

278. The legal measures under Recommendations 27 and 28 appear to be comprehensive, but certain elements under Recommendation 27 may not be fully effective. The statistics seem to indicate that while ML investigations have been initiated from STRs and other sources (see tables above) they have only resulted in 4 successful prosecution between 2004 and 14 November 2007 (see the table in section 2.5 of this report). In fact, Singapore pointed out that CAD has seized approximately SGD 150 million between 2004 and 14 November 2007, out of which only SGD 30 million belong to cases emanating from a domestic predicate offence. The fact that more money (SGD 120 million) was seized in relation to a relatively small number of identified foreign predicate offences could support the assessment team's assertion that foreign predicate offence forms of ML may be more prevalent in Singapore than otherwise indicated.

[19] Singapore considers these statistics to be money laundering investigations; however, the assessment team concluded that these are STR investigations, and the information gathered was usually used to decide whether or not to forward cases to other agencies to investigate predicate offences. They are not pure ML investigations *per se*.

279. Initially, it appears that insufficient attention was paid to pursuing ML offences, and the statistics suggest that, overall, the regime for investigating and prosecuting ML was not effective but that with recent changes some significant improvement has occurred over the last couple of years. This and other issues were raised in several meetings during the assessment, from which the following points were raised.

(a) The AGC indicates that 5 ML prosecutions are currently still waiting for court outcome.

(b) The AGC indicates that domestic ML prosecutions may not always appear in the statistics as money laundering since they are usually recorded as part of the predicate offence (*e.g.* offences related to money remitters).

(c) ML offences that involve the transiting of money etc through Singapore, where the offence has occurred in a foreign jurisdiction and the subject is also overseas may be recorded as a ML investigation (for the purposes of obtaining information for foreign jurisdiction), but the prosecution/conviction would not be recorded in Singapore.

(d) Singapore took the position that its low domestic crime rate means that there are a corresponding low number of ML offences. While this position could be supported for domestic crime, it may bear no relationship to the number of foreign enterprises using Singapore's well-developed and stable financial market as a possible ML transit or entry point. (See section 1.2 of this report for a discussion of APG Typologies studies of cases involving the laundering of proceeds of foreign predicate offence through Singapore.)

2.6.2 Recommendations and Comments

280. The Singapore authorities should more pro-actively target and pursue ML investigations in general, and make more use of STRs to investigate ML cases. Authorities should also target money laundering cases that are of a more international rather than domestic nature. Once the law enforcement authorities begin focusing on these issues, they should consider whether they have allocated sufficient resources to manage this work.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**LC**	• Effectiveness: low number of investigations for ML (most of which are investigations in concert with investigations of the predicate offence); little use made of STRs to investigate ML; inadequate proactive investigation of ML related to funds coming into Singapore from another jurisdiction.
R.28	**C**	• This Recommendation is fully observed.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

281. Singapore has had a disclosure system in place since November 2004. As of 1 November 2007 Singapore has also implemented a declaration system. The declaration system complements (rather than replaces) the disclosure system.

282. On 1 April 2003, the Immigration & Checkpoints Authority (ICA) was established by merging immigration control and clearance functions performed by the former Singapore Immigration & Registration (SIR) and the border enforcement work performed by the former Customs & Excise Department (CED). The formation of ICA created a single checkpoint command ensuring coordinated and effective response to any security threats. Police officers from other agencies like the SPF and

CNB are also deployed at the checkpoints, and are authorised to assist ICA officers in carrying out their revenue, excise and immigration duties (s.4(2)(g) PFA). ICA officers are not police officers, but are deemed to be public servants within the meaning of the Penal Code (s.37(3) Immigration Act and s.6 Customs Act). Together, police officers from the SPF and CNB, and officers from ICA and the Auxiliary Police Force, form an integrated force on border and security control.

Disclosure system

283. In November 2004, Singapore implemented a disclosure system on a targeted basis at border checkpoints. This system can be quickly implemented as ICA officers already routinely stop and check persons at the checkpoints to ensure that the movement of persons, goods and conveyance is legitimate. The disclosure system is based on the integration of ICA officers and police officers, and their co-ordinated use of customs, immigration and general police powers.

284. ICA officers are authorised to ask any person arriving or leaving Singapore questions concerning his/her identity, nationality, occupation, criminal history and means of support (s.8 and 28 Immigration Act), and questions concerning any goods being brought into or taken out of the country. "Goods" in this context is defined very broadly to include "all kinds of movable property" and is sufficiently broad to include currency and bearer negotiable instruments (CBNI) (s.3 Customs Act). Such provisions apply to goods that are being transported into or out of Singapore by a person or in containerised cargo.

285. Persons are obligated to fully and truthfully answer all such questions and inquiries. Failure to do so is an offence pursuant to the Immigration Act (s.28) and/or Customs Act (s.129). Using a targeted approach, ICA acts on both intelligence and suspicion, to conduct closer examinations of persons, goods and conveyances. ICA uses data-mining for better analysis of information on travel documents, travel movement, suspicious documentation and screening in co-ordination with law enforcement agencies within Singapore. ICA also deploys sophisticated x-ray, scanning and other technological equipment intended to detect items of security interest, contraband and prohibited items.

286. Both senior ICA officers and ICA specialists have extensive powers to stop, search and seize in relation to persons who are entering or leaving Singapore, by virtue of their appointment as officers of customs pursuant to sections 4(4) and 5(2) of the Customs Act. Anyone entering or leaving Singapore is subject to having their person, goods and baggage searched by an ICA officer on demand (s.109 Customs Act). When a person has been referred for closer examination and a sizable amount of CBNI is found on the person, the person is questioned by the ICA officers with a view to determining the person's identity and/or intent.

287. ICA officers can exercise their powers of arrest and search if they discover that a person has not fully or truthfully answered their inquiries (i.e. made a truthful disclosure). In particular, ICA officers are authorised to arrest without a warrant, and to search any person, premises, or vehicle if there is reason to believe that any evidence may be found of the commission of an offence under the Immigration Act (s.51) or Customs Act (ss.110, 112 and 128). These powers can be invoked where the offender being investigated is not fully and truthfully answering the inquiries of an ICA officer. If a false statement is made or there is suspicion about the person and/or his intentions, ICA officers refer the person to the police officers who are present and deployed at the checkpoints for further investigation. Police officers may also invoke their general powers of investigation, arrest and seizure in cases where a false disclosure has been made because refusing to answer the authorised questions of a public servant (including ICA officers) or deliberately providing a public servant with false information are Penal Code offences (s.179 and 177).

288. The police officers who form part of the integrated checkpoint force are authorised to investigate any suspicion of ML/FT as these are criminal offences pursuant to the CDSA and TSOFA. They also have the power to seize such monies (s.68 CPC) where there is suspicion of the commission of an offence. In addition, the TSOFA (*e.g.* s.11) allows the authorities to apply to a court to restrain

property that is related to terrorist financing. The authorities may also apply to a court to freeze the assets of any accused person who is being prosecuted for a ML offence (s.16 CDSA).

Information collected and retained

289. ICA collates and keeps information on all cases detected at the checkpoints for intelligence purposes, including cases involving false disclosures or where there is a suspicion of any offence (including ML/TF). The information obtained includes the type/amount of property involved and the full identification of the subject. Additionally, when the ICA has referred a case to another competent authority (such as the police) for further investigation (*e.g.* when there is suspicion of ML), that competent authority will, at a later stage, advise the ICA of the case outcome (*e.g.* warning, fine or prosecution). ICA uses this information to update its databases for later reference and/or intelligence. The ICA provides information concerning these cross-border disclosure cases directly to the FIU (STRO). As of 14 November 2007, 110 disclosures have been received by STRO. Additionally, the information collected by ICA would be sent to CAD for further financial investigations to determine the ultimate beneficiaries of the funds couriered into Singapore. Financial investigations would then be conducted to determine whether the funds are for legitimate purposes.

290. Singapore has a declaration system for physical cross-border transportations of currency or bearer negotiable instruments through the post. Sending CBNI via uninsured post is prohibited (s.3 Postal Services Regulations), but may be sent through insured post. Officers of the Postal Authority have similar powers to make inquires, arrest, search and seize as those described below in relation to ICA officers (s.46-48 Postal Services Act).

New declaration system

291. On 1 November 2007, Part VIA of the amended CDSA came into force, giving effect to Singapore's new cash courier declaration regime. The new declaration system applies to all incoming and outgoing movements of CBNI (collectively referred to in the legislation as "cash") above the threshold of SGD 30 000 (the equivalent of EUR 15 000). The declaration system applies to all of Singapore, including its free port.

292. All travellers must fully and accurately declare to an immigration officer any CBNI exceeding the threshold on a Cross Border Declaration Form (NP 727) (CDSA, s.48C). This reporting obligation also applies to any person who is moving CBNI into or out of Singapore through containerised cargo, the postal system, courier companies etc. A separate form (NP 728) must be filled out for such declarations. Additionally, any person within Singapore who receives CBNI exceeding the threshold amount from overseas is required to file a NP728 within five business days of receiving it (s.48E, CDSA).

293. Section 48F confers various powers on authorised officers and immigration officers for the purposes of Part VIA. An immigration officer or authorised officer may require any traveller who is arriving or leaving Singapore to declare whether he/she has with him/her any CBNI, and could require the traveller to complete the cross-border declaration form (s.48F(1)(i), CDSA). The traveller is obliged to complete the form and provide full and accurate information to the requesting officer. These powers are exercised on a targeted basis, based on intelligence or suspicion of the commission of an offence under the CDSA or under TSOFA. Apart from collecting the personal details of the travellers, the cross border declaration form also includes details relating to the origin of the CBNI and its intended use. Identification details of the person, including passport number, address and occupation are also captured. The traveller is also obliged to answer any question the immigration officer or authorised officer may have with respect to the CBNI (s.48F(1)(v), CDSA). This allows the immigration officer to enquire about its origin, source, destination and purpose (s.48F, CDSA).

294. In cases where there is a suspicion of ML/FT or a false declaration, the competent authorities are able to stop or restrain the CBNI for a reasonable time in order to ascertain whether evidence of ML/FT may be found. The same mechanisms as described above in relation to the disclosure system apply.

295. An authorised officer or immigration may seize CBNI in the event of a false disclosure. Section 48F(9) of the amended CDSA allows an authorised officer or immigration officer to seize the cash in cases where he/she has reasonable grounds to suspect that it may afford evidence as to the commission of an offence under section 48C. (Section 48C is the obligation to file a disclosure and that it "contain full and accurate information relating to the matter being reported as specified in the form.")

Information collected and retained

296. The information captured in the declaration form includes:

- The amount and type of CBNI declared.
- The purpose, source / beneficiary and intended use of the CBNI.
- The identification data of the bearer (including his name and passport number, date of birth, nationality, address and occupation).

297. This information collected is retained by the STRO. Various provisions under the amended CDSA (*e.g.* s.48C(5)(ii) and s.48E(5)(c)) require a declaration to be submitted to a Suspicious Transaction Reporting Officer, and other provisions require the information/form to be submitted to an immigration officer. A further provision allows for any information provided to an immigration officer to be provided, on request, to the STRO. This request for immigration information is provided to the STRO under a standing general order requiring it to be forwarded directly to the STRO in every case.

298. All information collected pursuant to the declaration regime is stored securely within STRO and made available to the relevant enforcement agencies, such as the specialised enforcement unit within CAD for the enforcement of the regime, the ICA and other relevant authorities pursuant to their investigative needs (see section 2.6 of this report for a description of this procedure). This includes matters relating to ML/FT, and the dissemination of police information reports relating to suspicious incidents involving unusual amounts of cash or precious metals. Where a case involving false declaration or suspicion of ML/TF is referred to an investigating authority the STRO is provided with a report outlining offence and outcomes (s.48C and s.48D of the amended CDSA).

299. The number of cross border reports is expected to rise with the implementation of the new declaration regime. As the declaration system is very new (effective 1 November 2007), its effectiveness cannot yet be assessed. Nevertheless, an inter-agency committee of all relevant stakeholders has been established to ensure its effective implementation (*e.g.* CAD, STRO, ICA, Maritime and Port Authority, Ministry of Transport (Air Transport Division), Ministry of Trade & Industry, Ministry of Foreign Affairs, Ministry of Defence, Civil Aviation Authority of Singapore, Infocomm Development Authority of Singapore (Postal movement), Police Divisions and the Singapore Tourism Board.

Domestic and international coordination and co-operation

300. Domestic co-ordination among customs, immigration and related authorities is facilitated by the merger of customs and immigration into a single authority (ICA), and its inclusion in the "Home Team" which brings together the ICA, law enforcement authorities (including the SPF and CNB) and other agencies with a view to encouraging close co-operation between these agencies (see section 6.1 of this report for details). The formation of ICA created a single checkpoint command ensuring coordinated and effective response to any security threats. A single command also facilitates sharing of critical intelligence, carrying out enforcement actions, as well as responding to incidents or security threats in a timely manner. ICA officers have powers under both the Immigration Act and Customs Act. ICA also has good working relations and coordination with the SPF as both agencies are under the same Ministry.

301. The ICA describes its international cooperation as a three tier system:

(a) High level conferences, *e.g.* ASEAN and Pacific Rim.

(b) Multi/Bi Lateral workshops, training visits and joint investigations which are used to build networks and develop relationships.

(c) Informal or intelligence sharing of information.

302. ICA has informal relations with foreign partners such as the network of liaison officers for cooperation on intelligence and operational matters. However, it does not currently have any MOUs or other forms of formal agreements with their foreign counterparts in other jurisdictions. However, with the enactment of the new CDSA provisions, information collected pursuant to Special Recommendation IX can now be shared through the MOU framework of STRO. Section 41 of the amended CDSA contains specific provisions relating to international co-operation in the context of the new declaration system. The Suspicious Transaction Reporting Officer is able to disclose anything communicated to him/her pursuant to section 48C and 48E of the amended CDSA to a corresponding authority (*i.e.* FIU) provided that thing may be related to an investigation by that authority into a drug trafficking offence or a foreign serious offence, and there is a cooperation arrangement or MOU in place. This means that STRO is now able to share the information collected pursuant to the declaration system with its existing MOU partners, subject to the terms of the MOU.

Sanctions for making a false disclosure

303. It is a criminal offence to refuse to answer questions, or give false information/documents (*i.e.* make a false disclosure) which may reasonably be required by an ICA officer acting in the capacity as an officer of customs (s.129 Customs Act). This offence is punishable by a fine not exceeding SGD 5 000 or imprisonment not exceeding 12 months or both. Likewise, it is also a criminal offence to resist or obstruct, actively or passively, any ICA officers in the execution of his/her duties pursuant to the Immigration Act (s.57(1)(g) Immigration Act). This offence is punishable by a fine not exceeding SGD 4 000 or imprisonment not exceeding 12 months or both. As well, making a false declaration to the Postal Authority (*e.g.* in relation to currency/BNI being sent through the post) is punishable by up to 12 months imprisonment and/or a maximum fine of SGD 5 000.

304. Additionally, two generic provisions under the Penal Code would apply to circumstance in which a false disclosure is made. First, it is an offence to omit to give notice or information to a public servant (such as ICA officer) when legally bound to do so. The penalty for this offence ranges from one month imprisonment and/or a SGD 500 fine, to six months imprisonment and/or a SGD 1 000 fine. It is also an offence to furnish a public servant with false information. The penalty for this offence ranges from six months imprisonment and/or a SGD 1 000 fine, to two years imprisonment and/or a SGD 1 000 fine. Singapore indicated that there have been no cases of false disclosure to date.

Sanctions for making a false declaration

305. The failure to declare or make a false declaration pursuant to Singapore's new declaration system is subject to sanctions of three years imprisonment and/or a maximum fine of SGD 50 000. Both the officer(s) of a legal person and the legal person itself can be found guilty of an offence committed by the body corporate under the CDSA if it is done with the consent, or connivance or neglect of the officer(s) (s.59 CDSA).

Sanctions for making a cross-border transportation related to ML/FT

306. A person found making a physical cross-border transportation of CBNI related to ML/FT could be convicted of the ML/FT offences set out in the CDSA and TSOFA, and subjected to the relevant criminal penalties (see sections 2.1 and 2.2 of this report for full details).

Seizing, freezing and confiscation

307. The provisional and confiscation measures set out in the CDSA and TSOFA apply to any person found making a physical cross-border transportation of CBNI related to ML/FT (see section 2.3 of this report for full details). Additionally, in the case of terrorist-related assets, persons dealing with such assets (including a cash courier making a physical cross-border transportation of such assets) could be guilty of an offence pursuant to the UN (ATM) Regulations which Singapore has implemented give effect to S/RES/1267(1999) and S/RES/1373(2001). Breach of this regulation is punishable under Section 5 of the United Nations Act, Cap 339. The general powers to seize assets under section 68 of the CPC can also apply in these situations.

Unusual cross-border movements of gold, precious metals or stones (Disclosure/declaration)

308. The ICA indicated that it has detected cases of unusual cross-border movements of gold, and has subsequently cooperated and/or shared information with the originating and destination jurisdictions. If ICA discovers an unusual cross-border movement of gold, precious metals or precious stones during the course of their work, inspections or investigations, its current practice is to also submit an intelligence report that is forwarded to the STRO via CAD. With the implementation of the new cross border declaration regime (effective in November 2007), ICA will additionally submit a suspicious transaction report to STRO in such cases.

Safeguards for protecting information

309. There are safeguards to prevent the unauthorised dissemination of information by authorised officers under section 56(1) of the CDSA. This duty extends to both ICA Officers (effective 1 November 2007, pursuant to the CDSA amendments) and Suspicious Transaction Reporting Officers from STRO. The abovementioned officers are not to disclose any information obtained in the course of their duties, except for purposes as indicated. A breach is punishable on conviction to a fine not exceeding SGD 2 000 and/or imprisonment for a term not exceeding 12 months. ICA Officers are also bound by the confidentiality provisions of the Official Secrets Act (OSA) (as described in section 2.6 of this report)

Additional elements

310. Singapore indicated that it is still in the early stages of implementing its declaration system but has implemented some of the measures in the Best Practices Paper. This includes the use of X-ray technology and other sophisticated equipment for the detection of CBNI, data-mining techniques, the observation of behaviour anomalies in targeting potential cash couriers, use of secured rooms by the ICA officers when conducting an examination/search, and the development of investigative guidelines. It will consider the measures in the Best Practices Paper to Special Recommendation IX in greater detail as the system matures.

Recommendation 30 (Resources of customs authorities)

311. ICA's presence at the borders is supported by the 6 line units - Woodlands, Tuas, Airport, Coastal, Ports and Air Cargo Commands. Each command is headed by a Commander, who is in turn supported by Deputy Commanders, Senior Assistant Commanders, Assistant Commanders and teams (comprising of junior officers headed by senior officers). Auxiliary police officers are also engaged to complement the existing manpower to ensure that security at the checkpoint is not compromised. ICA is appears adequately funded by MHA's budget in terms of manpower costs as well as in the planning and implementation of various projects / initiatives.

312. In terms of its technical capabilities, the following are some examples of the security initiatives that ICA has implemented to enhance checkpoints security.

(a) ***Integrated Cargo Inspection System (ICIS):*** ICA has deployed the ICIS, which comprises the radiographic scanners and radiation detectors, to enhance security at the land checkpoints in 2005. This has proven to be effective in detecting contrabands or specially constructed compartments in vehicles and ICA is taking steps to acquire more scanners to support its operations. The implementation of ICIS is an addition to the cohort of radiographic scanners deployed at the sea checkpoints since 2003.

(b) ***ZBackscatter Van (ZBV):*** It is a mobile X-ray inspection system built into a commercial delivery van. The ZBV is used to screen smaller vehicles, sea containers and conventional cargo, as well as individuals, for terrorist threats and contraband simply by driving alongside the object. The ZBV allows ICA the mobility to move about away from the fixed scanning stations. The ZBV is deployed at our sea and land checkpoints.

(c) ***Data Mining Technique:*** Data mining, or more accurately referred to as data analysis and computer-aided predictive profiling, involves the proactive profiling and targeting of travellers and vehicles with suspicious travel patterns in and out of Singapore, and to sieve them out for security checks.

313. ICA advised that it adheres strictly to its code of conduct and officers are constantly reminded to uphold the organisation's three values – Integrity, Accountability and Commitment. The code of conduct also reiterates the importance of confidentiality of information and all staff must not divulge secret, confidential or restricted information to any unauthorised person or agency. ICA officers are also expected to declare their financial health and other financial information on an annual basis. There are also strict rules on the acceptance of gifts and all gifts acquired would have to be declared to the superior. To maintain tight supervision at the ground, officers are required to jot down their deployment activities and the amount of cash held in their pockets books which are monitored by their supervisors.

314. All ICA officers are required to attend structured training on a regular basis. ICA's Training Branch oversees the formulation, implementation and review of training programmes for officers in ICA to develop the core competencies required for ICA to fulfil its mission so that officers can discharge their functions with confidence.

315. Within the ICA, information concerning the introduction of the new declaration system has been cascaded through management and middle level management meetings and dialogue sessions, to create awareness. ICA will also hold regular pre-shift team briefings and in-service training to prepare the ground officers for the implementation of this regime. CAD will also conduct a series of training sessions at the major checkpoints (*i.e.* Woodlands, Tuas, Airport and Coastal Divisions) to further raise awareness amongst ICA officers on how to differentiate between the types of CBNI. CAD has also provided ICA officers with a special tool kit containing essential information on the procedures to be adopted for various situations, tips on how to identify cash, list of frequently asked questions etc, to ensure that they are able to discharge their duties effectively. In addition, CAD has set up a hotline to field any queries that a person may have with respect to his reporting obligations.

Statistics and effectiveness

316. Effectiveness issues were raised by the assessment team concerning firstly the implementation and use of the disclosure system and secondly the newness of the declaration system where only one month of statistics can be used to evaluate effectiveness.

317. Singapore reported that in relation to SR.IX, it had a disclosure regime since Nov 2004 and that this system was used solely until the implementation and amalgamation with the new declaration system that came into place on 1 November 2007.

318. Pursuant to the disclosure regime, Singapore reported that between November 2004 and 14 November 2007, ICA officers detected 110 instances of cash couriers carrying a substantial amount in different currencies. In these cases, the cash couriers typically claimed to be working for money changers in Malaysia, South Thailand and Riau Islands in Indonesia, and that they were delivering the cash to money-changers in Singapore.

Reports received pursuant to the disclosure system	2005	2006	2007 (as at 14 Nov. 07)
Cross Border Movement Reports of CBNI	--	14	96

319. The results indicate there were no reports in 2004-2005, 14 reports for 2005-2006, and 96 reports for 2006 to 31 October 2007. These results seem low in relation to the relative risk of cash couriers bringing illicit funds into Singapore, and the huge volume of cross-border traffic. Over 9 million persons enter Singapore every year. Additionally, Singapore is one of the busiest cargo sea ports in the world. Typologies information has indicated that Singapore is at serious risk by cash couriers bringing illicit funds into Singapore. However, during the sole operation of the disclosure system, only 110 disclosures were reported to the FIU, no cases of ML-related cash couriers were detected, no cases of postal declarations were made to the FIU, and there were no instances in which suspicious CBNI were stopped or restrained.

320. The assessment team felt that the key issues relating to the disclosure regime are:

(a) The disclosure regime is not effectively implemented, specifically in areas that targeted cross border movement of cash and BNI's. The total quantity and the variation across the types of report appear insufficient.

(b) The long-standing disclosure regime for postal cargo is not effectively implemented, specifically in areas that targeted cross border movement of cash and BNI's.

(c) There is no evidence that the earlier disclosure system was effectively applied to target the cargo system.

(d) The disclosure regime did not adequately cover the risk of cash and BNIs being transported through cargo systems.

(e) The disclosure regime has not resulted in any detection of suspicious cash or BNI's, specifically those relating to ML or FT, nor in any seizure or confiscation.

(f) The disclosure regime has not used any of the sanctions available. There are no statistics relating to anyone having failed to disclose or to have untruthfully disclosed.

(g) Under the disclosure regime, there were no clear direction given to travellers entering or leaving Singapore that they will be required to make a truthful disclosure relating to cross border movement of cash and BNI's.

(h) ICA has informal relations with foreign partners such as the network of liaison officers for cooperation on intelligence and operational matters. However, it does not currently have any MOUs or other forms of formal agreements with their foreign counterparts in other jurisdictions and under the disclosure system could not formally share this information.

321. Although very new, the declaration system has in its first month of reporting started to produce results. The assessment team believes that this is mostly due to the preparation for and the implementation of the declaration system, where the relevant agencies had conducted several training sessions to frontline staff and briefings to the appropriate private industry stakeholders. A publicity advertising campaign had also been initiated, which included the distribution of leaflets on the new declaration system to travellers and structures built at strategic locations at all Singapore checkpoints.

322. From 1-14 November 2007, CAD received a total of 3 901 forms. During this period, the CAD has also conducted investigation into four cases of failure to report. This contrasts sharply with the results obtained, over the previous three years, from the disclosure regime. The breakdown of the statistics is provided below.

	Period from 1 November to 14 November 2007
Total Number of NP 727 (declarations made by travellers):	1 547[20]
Total Number of NP 728 (declarations relating to cargo and post):	2 354[21]
Total Number of Cash Movement Reports:	**3 901**[22]
Total Number of Investigations:	**4**[23]
Total Number of Ongoing Investigations	**4**[24]
Total Amount of Monies Seized / Frozen:	**SGD 70 000**

323. As stated previously, to evaluate the current systems in place it was necessary for the assessment team to examine the disclosure regime that had been in place for approximately three years and then to determine the probable effect of also having a new parallel declaration system. From the observations stated above, several major issues were raised by the assessment team about the implementation and effectiveness of the existing disclosure system.

324. However, in implementing the new declaration system, Singapore has technically covered these issues and based on the initial statistics provided for the first month the systems in place seem to cover the concerns raised by the evaluation team concerning the disclosure system. For the purposes of this evaluation however, the declaration system is technically only one month old, and it cannot be determined, at this stage, whether the implementation will be successful across all agencies or areas concerned and whether this implementation will be fully effective.

2.7.2 Recommendations and Comments

325. Due to the identified deficiencies in the disclosure regime, the authorities are recommended to make the new declaration system fully effective, ensuring that there is no confusion between coverage under the parallel disclosure and declaration systems. Attention should be given to ensuring that the customs authorities are adequately resourced and trained in the implementation of this system across all forms of border control. The authorities should ensure that their implementation of the declaration system, and continued use of the disclosure system, has a focus on the detection of ML/FT.

2.7.3 Compliance with Special Recommendation IX

	Rating	**Summary of factors relevant to s.2.7 underlying overall rating**
SR.IX	**LC**	• Effectiveness: As the declaration system is very recent and only one month of statistics has been provided, its effectiveness and implementation across all agencies cannot yet be fully assessed.

[20] 5 879 as of 31 December 2007.

[21] 9 670 as of 31 December 2007.

[22] 15 549 as of 31 December 2007.

[23] 9 as of 31 December 2007.

[24] 5 as of 31 December 2007.

3. PREVENTIVE MEASURES – FINANCIAL INSTITUTIONS

Preamble: Overview of the supervisory regime and application of AML/CFT measures

326. The Monetary Authority of Singapore (MAS) – the central bank and integrated regulator – exercises supervisory oversight responsibilities over the banking, insurance, securities and futures industries, money changers, remittance businesses, and trust companies through the MAS Act, Banking Act, Finance Companies Act, Insurance Act, Securities and Futures Act, Money-Changing and Remittance Businesses Act, Trust Companies Act, and Financial Advisers Act. MAS Notices and supervision cover nearly the entire financial sector and types of financial activity to which the FATF Recommendations are applicable – the only exception being commodities futures brokers[25].

327. MAS is empowered under the various regulatory statutes to issue directions to financial institutions, including the legal obligations to take preventive measures to help mitigate the risk of Singapore's financial system being used for ML/FT. Any such directions or regulations apply to all entities and institutions that are subject to MAS supervision and regulation.

328. The various classes of financial institutions are subject to similar obligations on customer due diligence (CDD), record keeping, STR reporting, internal control policies and procedures, the need for management level compliance function, audit and staff training in AML/CFT measures. Even those categories of persons who are exempt from licensing requirements (*e.g.* certain types of financial advisers) are still subject to the AML/CFT requirements that apply to their activity.

329. The assessment team concluded that the various AML/CFT requirements are being effectively implemented for a number of reasons. The firms interviewed were able to describe in detail their policies and procedures in relation to, *e.g.* high risk areas like PEPs and correspondent banking – and clearly took the possibility of regulatory enforcement action seriously. MAS can publish letters of reprimand on their public website, which also gives financial institutions a strong incentive to comply, for fear of reputational risk.

330. MAS applies a rigorous supervision regime of on-site inspections and off-site supervision to review for compliance with Singapore's AML/CFT regulations. Financial institutions interviewed confirmed that the MAS devoted huge resources to detailed examination of their firms, for weeks at a time, to look at various aspects of AML/CFT controls, covering vastly more ground than an auditor could cover.

331. MAS also provided to the assessment team detailed account of what their examiners would expect to find by way of effective controls in firms under inspection, as set out in the MAS inspection manual. Other factors to consider are the firm language of the Notices (using the language "shall" in each case), the fact that they are regarded as regulations universally by financial institutions, and a strong compliance culture reinforced by a zero tolerance policy for domestic crime.

Preamble: Regulations, Notices, and Guidance

332. The Singapore regulatory structure utilises laws ("Acts"), regulations, and notices, all of which are enforceable. Regulations, orders, declarations, and notifications are issued under the authority of the respective parent Act. They typically flesh out the provisions of an Act and spell out in greater detail the requirements for financial institutions or other specified persons. Regulations have the force of law and may specify that a contravention is a criminal offence. They are published in the Government Gazette.

[25] With effect from 27 Feb 2008, MAS assumed regulatory oversight of commodity futures: http://www.mas.gov.sg/legislation_guidelines/securities_futures/sub_legislation/Publication_of_MAS_Regulations_and_Notices_on_the_Transfer_of_Regulatory_Oversight_of_Commodity_Futures.html

333. The key distinction between regulations and notices lies in the process. By law, regulations must be published in the Gazette and vetted by the AGC. In addition to regulations, the Interpretation Act also defines "subsidiary legislation" to mean any order in council, proclamation, rule, regulation, order, notification, by-law or other instrument made under any Act, Ordinance or other lawful authority and having legislative effect. Section 23(1) indicates that subsidiary legislation must also be published in the Gazette. By virtue of the deeming provision described below, MAS Notices are excused from this requirement of vetting and publication in the Gazette. It was contemplated that because MAS Notices spell out very detailed and technical requirements for financial institutions and taking into consideration the rapid changes happening in the financial sector, MAS should be able to react quickly in order to keep pace with these changes. Apart from AML/CFT matters, for example, key prudential risk management measures (such as maintenance of minimum cash balance by banks) are also implemented via Notices. The function of issuing Notices is therefore specifically delegated to MAS as the financial regulator, who has the specialist knowledge and expertise to handle matters relating to the financial sector.

334. Sections 27A of the MAS Act gives the MAS the general authority to issue directions or regulations, while section 27B authorises MAS to issue directions or regulations specifically to combat ML/FT. Both are also used to detail specific requirements or instructions to financial institutions or persons. The MAS Notices issued pursuant to section 27B share key characteristics of legislation and subsidiary legislation in Singapore, *e.g.* that they (1) embody codes of conduct; (2) are of a general application rather than directed at specific individuals or situations; and (3) they are unilateral and have binding legal effect in that a criminal sanction can be imposed for any breach. They are also regarded by the Singapore authorities and financial sector as equivalent to regulations. However, the MAS Act specifies that notices issued pursuant to 27B are deemed to be not considered as subsidiary legislation. Therefore, the AML/CFT Notices, which establish most of the AML/CFT requirements for most financial institutions as described below, cannot be considered as subsidiary legislation or "law or regulation" according to the FATF definition. However, they are clearly "other enforceable means", as they create legally enforceable obligations, to which criminal sanctions apply for non-compliance. The exceptions are the new Rules for Moneylenders, which came into force on 12 November 2007, which are equivalent to regulations. In addition to criminal sanctions, a full range of administrative sanctions is available to MAS that can and have been applied for breaches of the AML/CFT Notices to fit the nature and severity of the non-compliance. Sanctions applied include criminal fines and revocation or non-renewal of licences, replacement of senior management, restriction on business expansion, requiring a review of AML/CFT system/operations, the taking of remedial actions or an increase of compliance resources, and reprimands. See section 3.10 for more details on the supervisory system and sanctions applied.

335. Guidelines set out principles or "best practice standards" govern the conduct of specified institutions or persons. While contravention of guidelines is not a criminal offence and does not attract civil penalties, specified institutions or persons are encouraged to observe the spirit of these guidelines. The degree of observance with guidelines by an institution or person may have an impact on MAS' overall risk assessment of that institution or person.

Customer Due Diligence & Record Keeping

3.1 Risk of money laundering or terrorist financing

Preamble: The Risk Based Approach to Supervision of Financial Institutions

336. The aim of MAS's risk-based supervision is to foster the safety and soundness of financial institutions (FI) and to promote transparency and fair dealing by FIs in relation to their customers and counterparties. These two supervisory objectives contribute towards MAS's overarching objective of a stable financial system. To facilitate these objectives, MAS developed an impact and risk model to allocate supervisory resources among institutions, and to distinguish those institutions that may pose a higher threat to the achievement of supervisory objectives. Each institution is assessed and assigned two ratings: (1) an impact rating which assesses the potential impact it might have on Singapore's

financial system, economy and reputation in the event of a significant mishap (*e.g.* financial or major control failure, and prolonged business disruption); and (2) a risk rating which assesses the likelihood of these significant mishaps occurring. Undertaking business activities deemed to be susceptible to ML/FT risks has a bearing on the institutions' overall risk assessment, and hence such institutions are subject to more intensive supervision and more frequent on-site inspections.

337. This impact and risk model is at the heart of the MAS supervisory framework. Within each financial services sector (banking, insurance and capital markets), the MAS first evaluates and rates the impact and risk of an institution relative to other institutions. It then uses a risk assessment, CRAFT (Common Risk Assessment Framework and Techniques), to evaluate the risk of an institution. The MAS then combines the assessments of impact and risk, and distinguishes those institutions that may pose a higher threat to the achievement of its supervisory objectives. Finally, the MAS determines the appropriate supervisory strategies and, in turn, the level of supervisory intensity required.

338. The impact and risk model considers the bearing of a FI within each financial services sector (*i.e.* relative systemic importance) and its risk (*i.e.* relative risk profile). These two critical inputs ensure that the intensity of supervision is proportionate to the institution's bearing on the achievement of MAS's supervisory objectives. Impact and risk ratings are combined to assign the institution to one of four categories ("buckets") of supervisory significance. Bucket 1 contains institutions that have the greatest potential to affect the achievement of MAS's supervisory objectives. In assigning buckets, the impact rating is accorded more importance relative to the risk rating. So, the model generally assigns a high-impact low-risk institution to a higher bucket than a low-impact high-risk institution, given the greater overall consequences should things go wrong at the high-impact institution.

339. The intensity of supervision varies according to the bucket. The variation is mainly in terms of the frequency of on-site inspections and the nature of the supervisory oversight of each FI. All FIs are subject to standard baseline monitoring of key indicators and business development, together with reviews of regulatory returns and audit reports. Lower bucket institutions receive only periodic on-site inspections and the MAS tends to rely on the work of external auditors to complement its supervisory efforts. As the buckets rise from 4 to 1, the resources allocated to supervision increase commensurately. MAS' oversight of the most systemically important bucket 1 institutions involves maintaining regular contact and the carrying out of on-site work to keep abreast of developments, including new business plans and strategy, changes in operations, risk management and systems and controls. These discussions typically include Board members, senior management, business heads, internal auditors and risk managers of the institution, as well as, in the case of overseas firms, its head office staff and home country regulators. In contrast, smaller institutions (*e.g.* financial advisers and insurance brokers) receive a lighter touch, in which they may not be risk-assessed individually or have a specific supervisory plan. Instead, they are subject to standard baseline monitoring, surveys and thematic reviews.

340. MAS's impact assessments take account of a number of qualitative factors and numerical measures, such as:

- Relative size and importance in terms of share of activity in different markets.
- Relative scale of retail reach, in terms of numbers of customers and representatives and of type of business.
- Criticality to the stable functioning of, and confidence in, the financial system.

341. The CRAFT risk assessment arrives at an Overall Risk Rating (ORR) for each institution. The ORR is based on an assessment of inherent risks and control factors, of oversight and governance arrangements, and of financial strength factors. A four-point rating scale – High, Medium High, Medium Low, and Low – is used to rate all components of the ORR.

342. The main elements of the CRAFT process are, in order:

- Identify significant activities ("SA").
- Assess inherent risks (credit/asset, liquidity, market, operational, technology, insurance, market conduct and legal/reputational/regulatory) and control factors (risk management systems and controls, operational management, internal audit, compliance) for each SA.
- Assess oversight and governance (Board of Directors, senior management, head office/parent company).
- Assess capital, earnings and parental support.

343. The propensity for an institution to be used for money laundering and terrorist financing activities is factored into the CRAFT process within the inherent risk category of Legal, Reputational and Regulatory Risk. The assessment of oversight and governance, and of the risk profiles of significant activities, generate the institution's risk profile, referred to as Institution Net Risk (INR) The INR reflects the effectiveness of risk control factors and of oversight and governance in mitigating the inherent risks of the institution's activities. The Overall Risk Rating of the institution is derived from combining the INR with an assessment of current capital and potential support, *i.e.* the financial resources available to the institution to absorb losses so as to ensure it remains solvent and able to meet its obligations to customers. A supervisory plan designed to address issues of supervisory concern identified through the risk assessment of the institution is then prepared. The plan guides the supervisory activities undertaken during the ongoing supervision of the institution and takes into account the given level of supervisory intensity. It is updated at regular intervals with new information obtained from ongoing supervisory activities.

344. To maintain a high degree of confidence in the quality of its supervision, MAS devotes considerable resources to training its staff and developing the breadth and depth of the expertise and experience of its risk and product specialists. MAS also has in place measures aimed at ensuring its supervision is carried out in a consistent manner. Those measures include:

- Comprehensive operating procedures to guide supervisory staff in key processes.
- A system of challenge and review by experienced supervisors or panels of senior and specialist staff for key supervisory assessments of individual FIs.
- Decision making on major regulatory or supervisory issues at senior management forums.
- Regular checks on the supervisory processes by MAS's internal audit function.

Preamble: Scope issues

345. The various MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism are wide-ranging in their coverage of the financial sector and so, with only one minor exception (commodities futures brokers), matches the definition of financial activity set out in the Forty Recommendations. The Singapore authorities, however, recognise the need to remove this exception and, consequently, the MAS intends to extend its AML/CFT requirements to commodities futures brokers in early 2008.

346. At the time of the on-site visit, the only relevant requirements imposed on commodities futures brokers and moneylenders were suspicious transaction reporting obligations under s.39 of the CDSA. However, the Moneylending (Prevention of Money Laundering and Financing of Terrorism) Rules 2007 (Moneylenders Rules), which came into force on 12 November 2007, now extend comprehensive AML/CFT requirements to moneylenders. As these measures are very new, however, it is not yet possible to assess the effectiveness of their implementation to moneylenders.

347. The MAS views both moneylenders and commodities futures brokers as relatively low risk for AML/CFT purposes, all being small firms and few in number. There were 151 moneylenders in the sector as of the end of August 2007. The loans by moneylenders totalled SGD 335 million, or only 0.07% of the banking sector lending business. Where commodity futures business is concerned, the six stand-alone brokers are expected to migrate to MAS supervision in 2008. These brokers conduct largely wholesale business, mainly trading in rubber futures. Their clientele are from within the physical rubber trading community. The brokerage revenue of the six commodity futures brokers account for 1% of the total brokerage revenues of CMS licensees trading in futures contracts. The MAS's policy line is to treat these small firms in the same way as broker-dealers who are currently subject to MAS supervision. The main risk of these entities being unsupervised is perceived to be that of illegal operators, fraudulently pretending to buy and sell commodities. Nevertheless, the remaining gaps in the scope of the AML obligations in relation to commodities futures brokers, and the inability to assess the effectiveness of the new measures in relation to moneylenders, affect the ratings relative to some of the Recommendations discussed in section 3. However, as this gap in scope is very narrow, the impact on the ratings is not significant.

348. The MAS Notices that impose obligations on financial institutions use almost identical language to that used by the FATF. This means that, overall, preventative measures for the financial sector generally meet a high level of compliance with the detailed provisions of the FATF 40 + 9 Recommendations. And, the fact that these Notices have the force of law, including criminal sanctions for non-compliance, leaves no room for doubt about whether such Notices constitute "other enforceable means". An explanation of the status of the AML/CFT notices is laid out in greater detail in paragraphs 333-334 above. So the main issue for consideration and comment is the effectiveness of implementation of the Recommendations.

3.2 Customer Due Diligence, Including Enhanced or Reduced Measures (R.5 to 8)

3.2.1 Description and Analysis

Recommendation 5 (Customer due diligence)

Anonymous accounts

349. MAS prohibits financial institutions from opening or maintaining anonymous accounts or accounts in fictitious names (MAS Notices on AML/CFT, Para. 4.1). MAS Notices require all financial institutions to perform the CDD measures for the opening and maintenance of all types of accounts. Where financial institutions identify customers by code or numbers internally, the identification records of such customers are available to relationship managers, compliance officers, auditors, other appropriate staff and competent authorities. The Notices fully cover the FATF Recommendations in this area. The Notices set out legally enforceable requirements with criminal sanctions for non-compliance. Although these Notices create legal obligations, they are "other enforceable means," and not "law or regulation" as required by the FATF. An explanation of the status of the AML/CFT notices is detailed in paragraphs 333-334 above.

When CDD is required[26]

350. **When establishing business relations:** MAS Notices require financial institutions to perform CDD measures when they establish business relations with any customer (MAS Notices on AML/CFT, Para. 4.2(a). For money-changers and remittance business licensees, this means that CDD measures must be performed when a relevant business transaction is undertaken on behalf of any customer. In the case of a money changer, a "relevant business transaction" is a money-changing transaction of an aggregate value not less than SGD 5 000 or an inward remittance transaction from another country or jurisdiction

[26] Financial institutions do not have to repeatedly perform identification and verification every time that a customer conducts a transaction.

to Singapore. For the holder of a remittance licence, a "relevant business transaction" is a cross-border remittance transaction to or from Singapore (MAS Notice 3001, Para. 4.1).

351. **When carrying out occasional transactions:** MAS Notices require financial institutions to perform CDD measures when they undertake any transaction of a value exceeding SGD 20 000 (approximately EUR 10 000) for any customer who has not otherwise established business relations with them. Money-changers must perform CDD when they undertake a money-changing transaction of an aggregate value of SGD 5 000 or more or when they operate an inward remittance transaction from another country or jurisdiction to Singapore. Remittance agents must perform CDD when they perform a remittance transaction from Singapore to another country or jurisdiction or from another country or jurisdiction to Singapore. In determining the value of a transaction, financial institutions are required to treat two or more transactions as a single transaction in cases where the financial institution suspects that the transactions are (or may be) related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions, in order to evade AML measures (MAS Notices 626, 1014, 824, SFA04-N02 Para. 4.30; MAS Notice 314 Para. 4.31; MAS Notice 3001 Para. 4.3). Financial institutions are also required to record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and the date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.[27]

352. The assessment team noted that the MAS gives no guidance to financial institutions on when to treat two or more transactions as linked, thereby triggering the customer identification obligation either because the sum of the transactions exceeds SGD 20 000 or because a series of transactions by the customer in effect constitutes a business relationship with the financial institution. The MAS declared itself satisfied that banks have the necessary transaction monitoring systems to pick up linked transactions, *e.g.* for cash transactions at the counter for occasional walk-in customers. However, this may not be true for all kinds of financial institution; some general guidance from the MAS would be appropriate.

353. **When carrying out wire transfers:** The provisions on wire transfers apply only to banks, merchant banks, finance companies, and remittance agents. The MAS explained that the wire transfer provisions apply only to these specified categories of financial institution because, for example, broker-dealers are obliged to carry out wire transfers through a bank as they are not permitted to undertake wire transfers as a regulated activity and are not part of Singapore's payment system. The ordering financial institution (which acts on behalf of the customer who is the originator of the transaction) is required to identify and verify the identity of the originator, and record adequate details of the wire transfer so as to permit its reconstruction. At a minimum, such details must include the date of the wire transfer; the type and amount of currency involved; the value date and details of the beneficiary of the transaction (*i.e.* the person to whom or for whose benefit the funds are being sent); and the beneficiary institution (*i.e.* the financial institution that will be receiving the funds on the account of the beneficiary (MAS Notices 626, 1014 Para. 9.3; MAS Notice 824 Para. 8.3; MAS Notice 3001 Para. 7.3). In a cross-border wire transfer exceeding SGD 2,000, the ordering financial institution must include the following details in the message or payment instruction that accompanies or relates to the wire transfer: the originator's name, account number (or unique reference number assigned by the ordering financial institution where no account number exists) and the originator's address (or, alternatively, a unique identification number, or date and place of birth) (MAS Notices 626, 1014 Para. 9.4; MAS Notice 824 Para. 8.4; MAS Notice 3001 Para. 7.4).

354. **When there is a suspicion of money laundering or terrorist financing, or when there are doubts about the veracity or adequacy of previously obtained customer identification data:** Financial institutions are also required to perform CDD measures when there is a suspicion of ML/FT, notwithstanding that they would otherwise not be required by law to perform CDD measures. Similar

[27] MAS Notices 626, 1014, 824, SFA04-N02 Para. 4.2(b) and Para. 4.29; MAS Notice 314 Para. 4.2(b) and Para. 4.30; MAS Notice Para 4.1 (a) and 2.1.

provisions apply if the financial institution has doubts about the veracity or adequacy of any information previously obtained.[28]

355. The obligations in the Notices for when CDD is required are generally broad and cover the vast majority of financial institutions. The Notices set out legally enforceable requirements with criminal sanctions for non-compliance. Although these Notices create legal obligations, they are "other enforceable means," and not "law or regulation" as required by the FATF. An explanation of the status of the AML/CFT notices is detailed in paragraphs 333-334 above.

Required CDD measures[29]

356. Financial institutions are required to obtain and record the customer identification information of both natural and legal persons. The information that must be recorded includes (but is not limited to) the following, where applicable:

(a) Full name, including any aliases.

(b) Unique identification number (*e.g.* identity card number, passport number, incorporation number or business registration number).

(c) Existing residential, registered or business address and contact telephone number(s).

(d) Date of birth, incorporation or registration.

(e) Nationality or place of incorporation or registration.

357. Financial institutions are also required to verify the customer's identity using reliable, independent sources and retain copies of all reference documents used to verify the authenticity of information provided on customer identity (MAS Notices on AML/CFT Para. 4.8 and Para 4.9; MAS Notice SFA13-N01 Para. 4.5).

358. **Natural persons:** Where the customer is a natural person, financial institutions are required to ask for some form of identification that contains a photograph of that person. In exceptional circumstances, where the financial institution is unable to retain copies of all reference documents used to verify the identity of the customer, the following information should be recorded:-

(a) Information that the original documentation had served to verify.

(b) The title and description of the original documentation produced for verification, including any particular or unique features, or condition of that documentation (*e.g.* damaged).

(c) The reasons why a copy of that documentation could not be made.

(d) The name of the officer who carried out the certification and a statement by the officer certifying that he has duly verified the information against the documentation and the date the verification took place.[30]

359. In practice, financial institutions use various methods for verifying the identity of natural persons. All permanent residents and citizens of Singapore must carry an identity card, which must contain their current address as well as a thumbprint and their National Register number. An

---

[28] MAS Notices 626, 1014, 824, 314, SFA04-N02 Para. 4.2 (c) and Para. 4.2 (d); MAS Notices FAA-N06, SFA13-N01, TCA-N03, Para. 4.2 (b) and 4.2 (c); MAS Notice 3001 Para. 4.1(b) and Para. 4.1 (c).

[29] The general rule is that customers should be subject to the full range of CDD measures. However, there are circumstances in which it would be reasonable for a country to allow its financial institutions to apply the extent of the CDD measures on a risk sensitive basis.

[30] MAS Guidelines 626, 1014, 824 Para. 23 and 24; MAS Guidelines SFA04-N02 Para. 25 and 26; MAS Guidelines FAA-N06 Para. 22 and 23; MAS Guidelines 314 Para. 21 and 22; MAS Guidelines TCA-N03 Para. 19 and 20; MAS Guidelines SFA13-N01 Para. 18 and 19.

alternative means of identification is via the Central Provident Fund (CPF). All employed citizens of Singapore are required to have a CPF account, and the CPF's records are generally reliable. An additional facility – aside from credit bureaux, which are generally used only for issuing of credit cards and for checking credit performance – is I-check online, for checking on permitted immigrants. For non-residents of Singapore, financial institutions tend to rely on passports and (Government issued) employment passes to verify identity. Employment passes can be linked back to the specific employer and the MAS expects FIs to check the validity of passes in this way. In addition, banks are able to use their overseas branches and subsidiaries, or seek bankers' references, to verify the identity of prospective non-resident customers.

360. **Legal persons and arrangements:** Where a customer is a legal person or arrangement, financial institutions are required to verify the due authority of the natural person(s) who are appointed to act on behalf of the customer in establishing business relations with the financial institution. The financial institutions are also required to identify and verify the identity of such person(s) using reliable, independent sources, such as official identification documents bearing the photograph of the person like passport(s), identification card(s), work permit(s) and employment passes, as well as retaining copies of all reference documents used to verify the identity of the said person(s). For the purpose of verifying the due authority of the natural person(s) appointed to act on behalf of the customer, the financial institutions are required to obtain, including but not limited to, the following:

(a) Appropriate documentary evidence that the customer has appointed the person(s) to act on its behalf.

(b) The specimen signatures of the person(s) appointed.

(MAS Notices on AML/CFT Para 4.10 to 4.12; MAS Notice SFA13-N01 Para 4.7-4.8)

361. Examples of the appropriate documentary evidence that may be used to verify the due authority of the natural person acting on behalf of the legal person or legal arrangement include an original company resolution duly signed by the directors, or a certified copy of the company resolution.

362. For the purpose of verifying the legal status of the legal person or legal arrangement, financial institutions are required to obtain and retain copies of specific reference documents used for the identification of the customer which include but are not limited to:

(a) Accounting and Corporate Regulatory Authority (ACRA) Business profile.

(b) Notice of Registration/Certificate of Confirmation of Registration (for Sole Proprietorship / Partnership).

(c) Notice of Incorporation/Certificate of Confirmation of Incorporation (For Company incorporated in Singapore).

(d) Certificate of Incumbency (For Company incorporated outside Singapore).

(e) Approval from appropriate Registrar or Government Gazette listing of an Association, Club or Society (For Association/Club/Society).

(f) Professional Practising Certificate (For Professional Firm, e.g. Clinic).

(g) Certified copy of Memorandum and Articles of Association.

(h) Certified extracts of Directors' Resolution.

363. Additionally, where the customer is a legal person, the financial institution is required to identify the relevant directors, partners or persons having executive authority in that legal person (MAS Notices on AML/CFT Para. 4.3 to Para. 4.7).

364. All companies, including foreign companies, that want to conduct business in Singapore, must be registered with ACRA. In practice, ACRA and three outsourced information providers for ACRA (see http://www.acra.gov.sg/information/serviceprovider.html) hold information on shareholders and directors of a company and its financial statements. Under the Companies Act, companies registered with ACRA are obliged to file their latest financial statements and there are penalties for not being up to date. Changes in ownership or in directors must also be reported to ACRA.

365. Where trusts are concerned, the obligation on FIs is to verify the identity of all "trust relevant parties", which means settlors/grantors, beneficiaries, and anyone with discretionary powers over the trust, *e.g.* an investment manager.

366. The list of acceptable documents for verifying the legal status of a legal person is not actually set out either in a MAS Notice or MAS Guidelines. The above list of documents is what MAS inspectors have commonly seen during their inspections. It would be helpful if the list was reproduced in MAS Guidelines.

367. Singapore has implemented comprehensive CDD measures in relation to the identification and verification of customers (natural persons and legal persons and arrangements), and any person purporting to act on behalf of a customer. These measures cover the vast majority of financial institutions and meet the requirements of Recommendation 5, but for the fact that the basic obligations are not laid out in law or regulation, as is required by the FATF Recommendations. Instead, they are contained in other enforceable means for which there are criminal penalties for non-compliance.

368. **Beneficial ownership:** Financial institutions are required to inquire if any beneficial owners exist in relation to a customer or, in the case of a trust company, any effective controllers. The term "beneficial owner" means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises the ultimate effective control over the customer. If there is a beneficial owner, the financial institution is required to take reasonable measures to obtain information sufficient to identify and verify the identities of the beneficial owners or effective controllers (MAS Notices on AML/CFT Para. 4.14 and 4.15).

369. Where the customer, settlor or trustee (where applicable) is not a natural person, the financial institutions are required to take reasonable measures to understand its ownership and control structure (MAS Notices on AML/CFT Para. 4.16). This includes identifying any directors, partners and persons having executive authority (MAS Notices on AML/CFT Para. 4.5 to 4.7).

370. Trust companies are specifically required to identify each trust relevant party. The term "trust relevant party" includes the settlor of the trust, the trustee, the beneficiaries and any person who has any power over the disposition of any property that is subject to the trust and with whom the trust company comes into business contact. Any effective controller must also be identified (i.e. the natural person who ultimately owns or controls a settlor or trustee, or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporated, in relation to a settlor or a trustee (MAS Notice TCA-N03 Para. 4.3, 4.14 and 4.15).

371. Approved trustees are required to identify each customer (*i.e.* the fund manager) who enters into negotiations or signs a trust deed with the approved trustee to act as trustee for a Collective Investment Scheme ("CIS") (MAS Notice SFA13-N01 Para. 4.3). Such inquiries need not be conducted if there exists any beneficial owner or effective controller in relation to a customer that is:

(a) A Singapore government entity.

(b) A foreign government entity.

(c) An entity listed on the Singapore Exchange.

(d) An entity listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements.

(e) A financial institution supervised by the MAS (other than a holder of a money changer's licence or a holder of a remittance licence; unless specifically notified by the MAS).

(f) A financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF. Or

(g) An investment vehicle where the managers are financial institutions supervised by the Authority; or incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by FATF (MAS Notices on AML/CFT Para 4.17 and 4.18).

372. The MAS has avoided being over-prescriptive about the approach that FIs should adopt to establishing ultimate beneficial ownership and effective control of a legal person. Instead, the MAS Notices refer to a requirement to "take reasonable measures" in this regard, which mirrors the FATF language. However, the main requirements for beneficial ownership are contained in the Notices. The Notices set out legally enforceable requirements with criminal sanctions for non-compliance. Although these Notices create legal obligations, they are "other enforceable means," and not "law or regulation" as required by the FATF. An explanation of the status of the AML/CFT notices is detailed in paragraphs 333-334 above.

373. While the MAS admitted that it is frequently asked about the number of layers of ownership and control that a FI should drill through to be satisfied that it has met its legal obligation, the broad answer given is that it should be as many layers as is necessary to reach a natural person or listed company, to find out who ultimately is "pulling the strings". In other words, the MAS expects regulated firms to exercise judgment in every case. This seems to be a prudent approach. In the assessment team's discussions with the private sector, the consistent message received from FIs was that their practice is to check as many layers of ownership/control as possible to arrive at the ultimate natural person. If this proves to be difficult, and in the absence of a compelling commercial reason for the legal person to have such a complex structure, the FIs will reject the business.

374. **Purpose of the business relationship:** When processing applications to establish business relations, financial institutions are required to obtain from the customer information as to the purpose and intended nature of business relations. Some of the information that can be obtained in this respect includes the occupation of individual customers, the nature of business of corporate customers, expected transaction volume, purpose of loan, source of funds and the arrangement of fund management (*e.g.* discretionary or advisory) (MAS Notices on AML/CFT Para. 4.19; MAS Notice 314 Para. 4.20).

375. **Ongoing due diligence:** Financial institutions are required to monitor business relations with customers or, in the case of a trust company, trust relevant parties on an ongoing basis.[31] When doing so, the financial institution must observe the conduct of the customers' accounts and scrutinise transactions to ensure that they are consistent with its knowledge of the customer (or trust relevant party), their business and risk profile and where appropriate, the source of funds. Given the nature of their business, for money changers and remittance agents, it is more meaningful to refer to a repeat customer and multiple business transactions than a business relationship. When they encounter repeat customers, they are required to review the earlier transactions undertaken by that customer to ensure that the current transaction is consistent with their knowledge of the customer (MAS Notice 3001 Para 4.19).

376. Discussions with the private sector confirmed that FIs have procedures in place to comply with the high level obligation in the MAS Notices to monitor customer activity. The nature of the monitoring varies according to the type and size of FI. Large retail banks tend to operate rules-based daily monitoring, with certain scenarios built in, that throw up alerts for operations staff to review.

[31] MAS Notices on AML/CFT Para.4.20; MAS Notice 314 Para. 4.21; MAS Notice SFA13-N01 Para. 4.9.

Others, in the securities and insurance markets, are likely to be more reliant on exception reporting for transactions that exceed specified thresholds (*e.g.* 3rd party payments over SGD 10 000).

377. The obligations in the Notices for on-going due diligence are generally broad and comprehensive. The Notices set out legally enforceable requirements with criminal sanctions for non-compliance. Although these Notices create legal obligations, they are "other enforceable means," and not "law or regulation" as required by the FATF. An explanation of the status of the AML/CFT notices is detailed in paragraphs 333-334 above.

378. Financial institutions are required to periodically review the adequacy of customer identification information that was obtained in respect of customers and beneficial owners, and ensure that the information is kept up to date, particularly for high risk categories of customers[32].

379. Customers or accounts in the higher risk categories such as the PEP category, will require enhanced due diligence and enhanced ongoing monitoring, including a higher frequency of review of the customer's account activities and adequacy of customer identification information. Financial institutions are expected to carry out such reviews annually. Such risk-based differentiation between the customers allows more attention to be directed to those that pose higher risks (at the point of account opening), as well as throughout the course of the business relationship. Furthermore, the risk-based differentiation facilitates better transaction analyses of higher risk customers. In this respect, MAS examines, among others, review of customer profiles/records and call reports.

380. For lower risk customers or accounts such as those categorised under consumer finance, financial institutions also conduct periodic update of customer information which may occur once in every two or three years, or when there is a significant transaction by a customer, or when there is a material change in the way the account is operated.

381. FIs adopt a risk-based approach to the frequency of review of CDD information for updating. For higher risk clients and products (e.g. PEPs and cash management business), the MAS expects that reviews will be undertaken at least annually. This practice seems to be followed, certainly in the banking sector, where the assessment team was told that medium risk customers would be reviewed every 18 months and lower risk customers at least every 3 years. If a customer's profile changed for any reason, it would normally trigger a review, unless the relevant relationship manager could explain the change. Such a review would entail a complete overhaul of the customer's KYC profile and risk rating. Not all requests for a new product or service would trigger a review, except where private banks were concerned, where suitability was an issue. (For conduct of business reasons, the bank needs to ensure that the customer understands the risk and investment objective of a new product.)

Risk

382. In general, financial institutions classify their customers into different risk categories, taking into account, *inter alia*, their country of origin, business dealings, background and/or profile (for example, someone who is identified as a PEP), source of wealth, profession, nature of business operations, account activities in relation to ML/FT concerns. In assessing ML/FT risk, financial institutions are advised to take into account factors such as the type of customer, the type of product or service that the customer purchases, and the geographical area of operation of the customer's business. Financial institutions are also encouraged to refer to, where practicable, other sources of information

[32] MAS Notices on AML/CFT Para. 4.24; MAS Notice 314 Para. 4.25; MAS Notice SFA13-N01 Para 4.12.

such as FATF and Financial Sector Assessment Program (FSAP) reports to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.[33]

383. **Enhanced CDD measures on high risk customers:** Financial institutions are required to perform enhanced CDD measures in relation to higher risk customers, business relations or transactions, based on the financial institutions' assessment of ML/FT risk. Examples of high risk customers include PEPs, companies registered or incorporated in a tax haven jurisdiction, money changers/remittance agents, charity organizations, shell companies and companies with bearer shares or nominee shareholdings. Also considered to be high risk are business relations and transactions with any person from or in countries and jurisdictions that are known to have inadequate AML/CFT measures, as determined by the financial institutions themselves or notified to financial institutions generally by MAS or other foreign regulatory authorities (MAS Notices on AML/CFT Para. 6.3 and 6.4).

384. The enhanced due diligence measures required to be performed on customers of higher risk categories are, but not limited to, the following:

(a) Implement appropriate internal policies, procedures and controls to determine if a customer, beneficial owner, trust relevant party or effective controller of a settlor or trustee (in the case of a trust company), is a politically exposed person.

(b) Obtain approval from senior management to establish or continue business relations where a customer, beneficial owner, trust relevant party or effective controller of a settlor or trustee (in the case of a trust company) is a politically exposed person or subsequently becomes a politically exposed person.

(c) Establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer, beneficial owner, trust relevant party or effective controller of the settlor or trustee (in the case of a trust company).

(d) Conduct enhanced ongoing monitoring of business contacts with the customer or trust relevant party (in the case of a trust company) during the course of business relationship through periodic reviews of transactions for any suspicious transactions and the adequacy of the customer identification which may include business ownership, occupation, source(s) of funds and transaction activities (MAS Notices on AML/CFT Para. 6.2).

385. The major banks have in place well-developed processes for risk assessing customers, both at account opening and on an ongoing basis. These risk assessments take account of geographical, product and business risks, for different types of customer. Indeed, in one bank, each customer facing business unit has its own set of CDD procedures, as each unit provides different products and services and deals with different types of customer. The business is responsible for effectively documenting a customer's source of funds, source of wealth, transaction profile and corroborating evidence. This provides a sound basis for effective transaction trend monitoring. From the assessment team's discussions with the non-bank private sector, it was not apparent that similar procedures were followed there.

386. **Simplified CDD measures on low risk customers:** Financial institutions are generally required to apply the full range of CDD measures to all of their customers, including the requirement to identify the beneficial owner. However, financial institutions (other than holders of a money-changer's or remittance business licence) are allowed to perform simplified CDD measures as they consider adequate to effectively identify and verify the identity of the customer, trust relevant party, a natural person appointed to act on the customer's behalf, any beneficial owner, and any effective controller of the settlor/trustee (where applicable), provided that they are satisfied that the ML/FT risks are low (MAS Notices on AML/CFT, Para 5.1).

[33] MAS Guidelines on AML/CFT Para. 50 to 52; MAS Guidelines SFA04-N02 Para. 53 to 55; MAS Guidelines FAA-N06 Para. 49 to 51; MAS Guidelines 314 Para. 47 to 49; MAS Guidelines 3001 Para. 37 to 39; MAS Guidelines TCA-N03 Para. 41-43.

387. Before applying simplified CDD measures, financial institutions should assess the ML/FT risks, having regard to the circumstances of each case, and such measures should be commensurate with the financial institutions' own risk assessment.[34] MAS Notices and Guidelines provide examples of when simplified CDD measures may be applied by the financial institutions, which are as follows:

(a) Where the customer is a financial institution supervised by MAS (other than a holder of a money changer's licence or a holder of a remittance licence, unless specifically notified by MAS) (MAS Notices on AML/CFT Para. 5.3).

(b) Where reliable information on the customer is publicly available to the financial institution.

(c) The financial institution is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of previous course of dealings. Or

(d) The customer is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by FATF, or a listed company that is subjected to regulatory disclosure requirements.[35]

388. Where MAS Notices and Guidelines provide that financial institutions may perform simplified CDD measures, financial institutions that do so are required to document the details of its risk assessment and the nature of the simplified CDD measures (MAS Notices on AML/CFT Para. 5.4). The rationale for allowing financial institutions to perform simplified CDD measures in the above examples is because adequate AML/CFT checks and controls are already provided for through other means. With reference to examples (a), (c) and (d) above, since financial institutions licensed by MAS are subject to the same standards of AML/CFT regulations as well as supervised for compliance with those requirements, they are deemed to have lower AML/CFT risk. The same may be said of overseas financial institutions that are subject to AML/CFT requirements equivalent to and consistent with those of FATF Recommendations and are duly supervised by their home authorities. As such, when financial institutions are dealing with one another, simplified CDD measures may be used for expediency on the basis that sufficient checks and controls against money laundering and terrorist financing already exist.

389. With reference to example (b) above, the rationale is that AML/CFT risk is implicitly lower for public companies and government bodies or enterprises, as compared to private companies, partnerships and sole proprietorships. This is because public companies are subject to regulatory disclosure requirements and much of the information relating to public companies and government entities is made available publicly and/ or independently checked by exchanges, external auditors and the Auditor-General respectively.

390. Holders of a money-changer's or remittance business licence are prohibited from performing simplified CDD measures in relation to the customer, natural person appointed to act on behalf of the customer or beneficial owner, except with the prior written approval of MAS which may attach such conditions and qualifications as it thinks fit. MAS may refuse to grant approval if the ML/FT risk is high and the simplified CDD measures proposed by the licensee will not effectively identify and verify the identity of the customer, natural person appointed to act on behalf of the customer or beneficial owner. To date, MAS has not given such approval to any licensee (MAS Notice 3001 Para. 5.1).

391. In the course of inspections of financial institutions, MAS samples account opening files and account review documents to assess the quality of their risk assessment and justification for conducting simplified CDD measures.

---

[34] MAS Guidelines 626, 1014, 824 Para. 46; MAS Guidelines SFA04-N02 Para. 49; MAS Guidelines FAA-N06 Para. 45; MAS Guidelines 314 Para. 43; MAS Guidelines TCA-N03 Para. 37.

[35] MAS Guidelines 626, 1014, 824 Para. 47; MAS Guidelines SFA04-N02 Para. 50; MAS Guidelines FAA-N06 Para. 45; MAS Guidelines 314 Para. 44; MAS Guidelines TCA-N03 Para. 38.

392. Overall, the MAS Guidelines for different categories of FIs give adequate guidance on the circumstances in which it would be appropriate to apply simplified due diligence. Financial institutions are prohibited from performing simplified CDD measures in relation to customers that are from or in countries and jurisdictions that are known to have inadequate AML/CFT measures, as determined by the financial institution for itself or notified to financial institutions generally by MAS or by other foreign regulatory authorities (MAS Notices on AML/CFT Para. 5.2).

393. The MAS Notices allow FIs to perform simplified CDD where they are satisfied that the ML/TF risks are low, with the proviso that simplified CDD may not be applied to customers from jurisdictions known to have inadequate AML/CTF standards. This does not entirely square with the requirements of Recommendation 5, read in isolation. However, the MAS Guidelines (para. 47c) make clear that simplified CDD is acceptable where the bank knows that the customer is a FI from a country where satisfactory AML/CTF standards are applied. Nevertheless, the FATF Recommendations on allowing simplified due diligence refer to the country making the decision as to where simplified due diligence can be applied as to whether it is satisfied about the other country's AML/CFT controls, and not specifying that the FI will make this decision.

394. The simplified CDD provisions in the MAS Notices (paras. 5.2 – 5.4) do not specify that simplified CDD measures are not acceptable whenever there is suspicion of ML or TF. The only relevant, and partial, non-application is contained in para. 4.17 of the Notices, where a FI is absolved of any responsibility for establishing the beneficial ownership of certain categories of low risk customer, unless there is any suspicion of ML/TF.

Timing of verification

395. Financial institutions are required to complete verification of the identity of the customer and beneficial owner before they establish business relations or undertake any transaction for the customer (in instances where the customer does not yet have a business relationship with the financial institution) (MAS Notices on AML/CFT Para. 4.31; MAS Notice FAA-N06 Para. 4.29; MAS Notice 314 Para. 4.32).

396. Specifically for holders of a money-changer's or remittance business licence, the requirement concerning the timing of verification of the identity of the customer and beneficial owner is stricter. Such financial institutions can only carry out business transactions when there is face-to-face contact with the customer (except with the prior approval in writing of MAS). To date, MAS has neither given such approval nor detected any case of non-compliance with such requirement (MAS Notice 3001 Para. 4.22).

397. Trust companies are required to identify each trust relevant party with whom the trust company comes into business contact as follows:

(a) In respect of the settlor of the trust, before the trust is constituted.

(b) In respect of each beneficiary of the trust, as soon as practicable after the beneficiary becomes identifiable, and in any case before making a distribution to that beneficiary.

(c) In respect of any other trust relevant party, as soon as practicable after the trust company first comes into business contact with that trust relevant party (MAS Notice TCA-N03 Para. 4.3).

398. Financial institutions (other than holders of a money-changer's or remittance business licence, trust companies and approved trustees) may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner only if:

(a) The deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations.

(b) The ML/FT risks can be effectively managed by the financial institution.[36]

399. Holders of a money-changer's or remittance business licence, trust companies and approved trustees are not permitted to delay CDD measures in this manner. An example where it may be essential not to interrupt the normal course of business would be with respect to securities trades or investment transactions, where market conditions are such that the financial institution has to execute transactions for the customer very rapidly. Business relations may also be completed before verification in non-face-to-face transactions, provided the risk can be effectively managed.[37]

400. Where business relations are established before verification of the identity of the customer or beneficial owner, the financial institution is required to complete such verification as soon as reasonably practicable (MAS Notice 626, 1014, 824, SFA04-N02 Para. 4.33; MAS Notice FAA-N06 Para 4.31; MAS Notice 314 Para. 4.34).

401. Financial institutions are only permitted to establish business relations with a customer prior to verification if they can effectively manage the ML/FT risk.[38] In practice, during its inspections, MAS expects that, in such cases, the financial institution has adopted internal policies, procedures and controls which set appropriate limits on the financial services being made available to the customer before the verification process is completed. Such measures include monitoring the account activities and limiting the types of transactions which can be done by the customer (*e.g.* limiting the amount of funds accepted, only accepting incoming funds into such accounts and prohibiting any withdrawal or payment transactions until the CDD measures are satisfactorily completed within a specific period). Such measures should be approved by the management of the financial institutions, for which the records must be properly maintained and filed in the customers' files (MAS Guidelines 626, 1014, 824 Para. 38; MAS Guidelines SFA04-N02 Para. 41; MAS Guidelines FAA-N06 Para. 37; MAS Guidelines 314 Para. 35).

Failure to satisfactorily complete CDD

402. Where the financial institution is unable to complete CDD measures, it is required to terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR. Additionally, the financial institution should document the basis for its determination, particularly where the customer decides to withdraw a pending application to establish business relations or a pending transaction, to terminate existing business relations or is otherwise reluctant, unable or unwilling to provide the information requested by the financial institution.[39] These requirements apply also when the business relationship has already started.

Existing customers

403. Financial institutions are required to perform CDD measures as appropriate to their existing customers, trust relevant parties or business contacts (where applicable) having regard to their own assessment of materiality and risk.[40] In relation to existing accounts (*i.e.* those to which CDD measures

---

[36] MAS Notices on AML/CFT Para. 4.32(b); MAS Notice FAA-N06 Para. 4.30(b); MAS Notice 314 Para. 4.33(b).

[37] MAS Guidelines 626, 1014, 824 Para. 37; MAS Guidelines SFA04-N02 Para. 40; MAS Guidelines FAA-N06 Para. 37; MAS Guidelines 314 Para. 34.

[38] MAS Notice 626, 1014, 824, SFA04-N02 Para. 4.32; MAS Notice FAA-N06 Para. 4.30; MAS Notice 314 Para. 4.33.

[39] MAS Notice 626 Para. 4.34 and Para. 11.3; MAS Notice 1014 Para. 4.34 and Para. 11.3; MAS Notice 824 Para. 4.34 and Para. 10.3; MAS Notice SFA04-N02 Para. 4.34 and Para. 9.3; MAS Notice FAA-N06 Para. 4.32 and Para. 9.3; MAS Notice 314 Para. 4.35 and Para. 9.3; MAS Notice 3001 Para. 9.3; MAS Notice SFA13-N01 Para. 6.3.

[40] MAS Notice 626 Para. 4.36; MAS Notice 1014 Para. 4.36; MAS Notice 824 Para. 4.36; MAS Notice SFA04-N02 Para. 4.36; MAS Notice FAA-N06 Para. 4.34; MAS Notice 314 Para. 4.36; MAS Notice 3001 Para. 4.25; MAS Notice TCA-N03 Para. 4.29; MAS Guidelines TCA-N03 Para. 32.

had not previously been applied in accordance with the MAS Notices), financial institutions are required to perform CDD measures in the following situations:

(a) There is a transaction which is significant, having regard to the manner in which the account is ordinarily operated.

(b) There is a substantial change in the financial institutions' own documentation standards in relation to the customer or trust relevant parties.

(c) There is a material change in the way that business relations or business contacts with the customer or trust relevant parties are conducted.

(d) The financial institution becomes aware that it may lack adequate identification information on a customer or trust relevant party.

(e) The financial institution becomes aware that there may be a change in ownership or constitution of the customer/trust relevant party, or the person/s authorised to act on behalf of the customer or trust relevant party in its business relations with the financial institution.[41]

404. The FATF requirement to apply CDD measures to existing customers if they are customers who had anonymous accounts is not applicable. The MAS informed the assessment team that the prohibition on anonymous accounts was previously contained in s.56 of the old Banking Act, so there are no legacy accounts in existence.

Effectiveness:

405. Overall, the CDD requirements are being implemented effectively. The MAS Notices implement nearly all aspects of Recommendation 5, which are supported by criminal sanctions for non-compliance. The assessment team observed a high level of compliance culture among the various financial institutions; FIs had a strong understanding of the CDD obligations, including implementing the beneficial ownership requirements.

406. Financial institutions turn away potential customers for various reasons, such as the customers' failure to meet client acceptance criteria which typically includes the country of origin of the customer. The MAS has observed, in the course of their inspections, that financial institutions have in place enhanced CDD procedures to assess clients from higher risk jurisdictions and will accept or reject clients based on their assessments or policies. Where relevant, financial institutions take additional steps such as requiring referrals before account acceptance and requiring background checks by investigation agencies.

Recommendation 6 (Politically exposed persons)

407. Financial institutions are required to implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person (PEP). Financial institutions are expected to have policies defining the customer acceptance criteria, such as a description of customers that are likely to pose a higher than average risk. In formulating such policies, factors such as a customer's background, country of origin, public or high profile position and other risk indicators should be taken into account.[42]

---

[41] MAS Guidelines 626 Para. 43; MAS Guidelines 1014 Para. 43; MAS Guidelines 824 Para. 43; MAS Guidelines SFA04-N02 Para. 46; MAS Guidelines FAA-N06 Para. 42; MAS Guidelines 314 Para. 40; MAS Guidelines TCA-N03 Para. 34.

[42] MAS Guidelines on AML/CFT Para. 6; MAS Guidelines 626, 1014, 824 Para. 49; MAS Guidelines SFA04-N02 Para. 52; MAS Guidelines FAA-N06 Para. 48; MAS Guidelines 314 Para. 46; MAS Guidelines 3001 Para. 36; MAS Guidelines TCA-N03 Para. 40.

408. MAS has observed that, in meeting these requirements, financial institutions often seek relevant information from sources other than the customer. The sources include: (i) the internet, on which searches are carried out; (ii) electronic databases on PEPs which are commercially available through subscription; (iii) other publicly-available information service providers; (iv) information available on in-house databases; and (v) information provided by head office or other branches.

409. Financial institutions are required to obtain approval from the financial institution's senior management to establish or continue business relations where the customer is a PEP or subsequently becomes one.[43]

410. In relation to PEPs, financial institutions are required to establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or the beneficial owner. Additionally, they are to conduct enhanced monitoring of business relations with the PEP: MAS Guidelines on AML/CFT Para. 6; MAS Guidelines 626, 1014, 824 Para. 49; MAS Guidelines SFA04-N02 Para. 52; MAS Guidelines FAA-N06 Para. 48; MAS Guidelines 314 Para. 46; MAS Guidelines 3001 Para. 36; MAS Guidelines TCA-N03 Para. 40.

Additional elements

411. The PEP requirements do not apply to domestic PEPs.

Effectiveness

412. The provisions of R.6 are fully reflected in the various MAS Notices to FIs and so are legally enforceable obligations. However, the scope issue described above (in the preamble to Section 3 of this report) reduces the rating to largely compliant. Overall, the requirements concerning PEPs are being implemented effectively. Discussions with the private sector revealed that FIs in Singapore are well-seized of the risks, to their reputation and franchise, of doing business with PEPs. One institution, for example, said that its members were well aware of the regulatory action taken against a bank in the USA, relating to PEPs.

413. Foreign FIs operating in Singapore would treat Singapore customers as PEPs, whereas local Singapore banks knew their customer base sufficiently well for there to be no need to conduct enhanced due diligence on local PEPs. All FIs check prospective customers (both natural and legal persons) for PEP status, against commercial databases, at the account opening stage and periodically thereafter. The frequency of such screening is for individual FIs to decide. The MAS told us that it had seen examples of screening undertaken as often as half-yearly: typically, however, it was done annually. Furthermore, any negative publicity – or an MAS warning – about a particular individual would usually trigger additional screening.

414. Financial institutions with an international presence, often make use of their expertise abroad (*e.g.* in the PEP's home country) when deciding whether or not to take on a client who is a PEP. For instance, the assessment team was told by one major international bank that it was rolling out a new activity form to cover source of funds and source of wealth. Because of that bank's extensive presence in every country across the Asia-Pacific region, it was well placed to validate the customer's explanations on the activity form, through enquiries made of its country officers. If any negative information was received from those enquiries, the bank was most unlikely to accept the prospective customer. And, if there should be any disagreement between the front office and compliance about customer take-on, there was a well established internal escalation process for taking the final decision.

[43] MAS Notice 626 Para. 6.2; MAS Notice 1014 Para. 6.2; MAS Notice 824 Para. 6.2; MAS Notice SFA04-N02 Para. 6.2; MAS Notice FAA-N06 Para. 6.2; MAS Notice 314 Para. 6.2; MAS Notice 3001 Para. 6.2; MAS Notice TCA-N03 Para. 6.2.

415. In the course of its inspections, MAS will review the policies and procedures of the financial institutions on PEPs, including their criteria for classifying clients as such. MAS will ascertain whether the senior management and independent control units are involved in the approval of PEP accounts. In addition, MAS assesses the level of the enhanced monitoring of PEP's transactions and check whether the reviews of PEP accounts are conducted on a regular basis. When the examiners sample the accounts for review, they will also determine that accounts of PEPs are classified accordingly. MAS has issued guidance to its examiners on the review of high risk accounts, including PEPs, in the AML/CFT Inspection Manual.

416. Generally, through the enhanced measures in the monitoring of PEP accounts and transactions, financial institutions will file STRs whenever suspicion arises or when adverse news on the PEPs is known. Statistics for STRs in relation to PEPs filed by the financial institutions are as follows:

	2005	2006	2007 (as at 14 Nov.)
STRS relating to PEPs filed by financial institutions	2	9	33

Recommendation 7 (Correspondent banking)

417. The only financial institutions in Singapore that engage in correspondent banking are banks and merchant banks. Therefore, although commodities futures brokers are not subject to AML/CFT obligations, that has no impact for this Recommendation. As explained above in the discussion of CDD obligations, other FIs, like broker-dealers in securities, are unable to effect cross-border payments so Recommendation 7 does not apply to this section in the Singapore context.

418. The provisions of R.7 are fully reflected in the relevant MAS Notices, to banks and merchant banks, and so are legally enforceable obligations. When providing cross-border correspondent banking services (*i.e.* correspondent banking services provided to a bank or financial institution that is operating outside Singapore), financial institutions are required to assess the suitability of the respondent institution (*i.e.* the bank or financial institution outside Singapore to whom correspondent banking services in Singapore are provided). This assessment is made by gathering adequate information about the respondent institution to understand fully the nature of its business, including making appropriate inquiries on its management, major business activities, and the countries or jurisdictions in which it operates. Financial institutions are also required to assess the suitability of the respondent institution by determining from any available source, including publicly available information, the reputation of the respondent institution and, as far as practicable, the quality of supervision over the respondent institution, including where possible whether it has been the subject of a ML/FT investigation or regulatory action (MAS Notice 626 Para. 8.3(a)(i) – Para 8.3(a)(ii); MAS Notice 1014 Para. 8.3). Sources for obtaining relevant publicly available information include annual reports of the respondent institution, reports from rating agencies such as Fitch, Moody's and Standard & Poor's, information providers like Bloomberg, Reuters and other newswire services, results from searches (*e.g.* for regulatory actions taken on the respondent institution) through the internet and the overseas networks of the financial institutions.

419. Financial institutions are required to assess the respondent institution's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent institution operates (MAS Notices 626, 1014 Para 8.3(a)(iii)). To meet this obligation, financial institutions usually send a questionnaire to the respondent institution to inquire into its compliance with the 40+9 Recommendations, controls and processes as well as risk awareness. In particular, banks should be aware of the possible risks relating to opening correspondent bank accounts and their policies and procedures should highlight these risks. For example, banks should be aware of those respondent banks which are situated in jurisdictions where they have no physical presence. Banks must also exercise due diligence and assess the level of perceived risk associated with each respondent bank and apply enhanced due diligence on banks from higher risk jurisdictions.

420. Financial institutions are required to obtain approval from their senior management to provide new correspondent banking services (MAS Notices 626, 1014 Para. 8.3 (c)). Financial institutions providing cross-border correspondent banking services are required to document the respective AML/CFT responsibilities of each institution (MAS Notices 626, 1014 Para. 8.3(b)).

421. There are currently no payable-through accounts in Singapore (i.e. an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf). Nevertheless, there are provisions in place to deal with such accounts. Where the cross-border banking services involve a payable-through account, the financial institution is required to be satisfied that: (1) the respondent bank has performed appropriate CDD measures on the third party having direct access to the payable-through account; and (2) the respondent bank is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide customer identification to the correspondent bank upon request (MAS Notices 626, 1014 Para. 8.4).

Effectiveness

422. Discussions with several banks indicated a good level of compliance with their obligations in this area. The MAS indicated that Singapore banks generally ask to look at the AML/CTF policies and procedures of their respondents and often risk rate those correspondents accordingly. The banks either themselves carry out due diligence visits to prospective respondents or use the services of their local offices (in the respondent's jurisdiction) to gather relevant information. With regard to assessing the quality of AML/CFT supervision in the respondent's home country, the MAS said that a view could be sought from a bank's local office, if it had one. Alternatively, useful source material was available to banks from published IMF FSAP reports and FATF evaluations.

423. The banks broadly confirmed what the MAS had said. They did not rely simply on sending questionnaires to their respondents to gather information about the latter's AML/CFT controls. Rather, they adopted a "Know Your Respondent" approach, whereby the bank's own Financial Institutions Group actually visited the respondent bank in order to get a feel for the strength of the respondent's own customer due diligence measures and its overall business. Once the respondent bank had been taken on, compliance staff would be responsible for monitoring activity over the correspondent account. As regards assessing the quality of AML/CFT supervision of respondents, the banks took the view that financial institutions in FATF member countries are adequately supervised for AML/CFT. Otherwise, the banks would look for whatever relevant information they could find, including country risk profile reports that are available through commercial providers.

Recommendation 8 (Technological developments and non-face-to-face transactions)

424. MAS AML/CFT Notices[44] require financial institutions to take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls. The same requirement is imposed on moneylenders (Rule 5(3) Moneylending Rules); however, these requirements for moneylenders (in force as of 12 November 2007) are too recent to allow the effectiveness of their implementation to be assessed. The MAS's circulars dealing with the risks inherent in Internet banking technology are relevant in this area.

425. MAS issued the “Internet Banking Technology Risk Management Guidelines” in June 2001 (Cir. No. FSG 13/2001) to require banks to adopt risk management principles and security practices, such as the deployment of strong cryptography and key management practices to protect customer PINs and information to reduce the risk of the misuse of technological developments in ML/TF schemes. Since 2003 MAS has been encouraging banks to adopt two-factor authentication for internet banking following a surge in security incidents involving the capture or misappropriation of customer PINs by

[44] MAS Notices 626, 1014, Para. 12.3; MAS Notice 824 Para. 11.3; MAS Notices SFA04-N02, FAA-N06, 314, 3001, TCA-N03, Para. 10.3; SFA13-N01, Para. 7.3.

cyber hackers. In November 2005, MAS issued the circular "Two-Factor Authentication for Internet Banking" (Circular No. SRD TR 02/2005) to require banks to implement two-factor authentication at login for all types of internet banking systems by December 2006. In addition, banks were asked to consider requiring the repeated use of the second authentication factor by the customer for high risk transactions or for changes to sensitive customer data during a login session. These publications are available on the MAS website.

426. Greater care is required to be exercised by the financial institutions if face-to-face verification at the account opening stage is not possible. Where there is no face-to-face contact, the financial institution is required to carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.[45]

427. Financial institutions must implement policies and procedures to mitigate the risks associated with non-face to face business relations or transactions when establishing customer relationships and when conducting ongoing due diligence. The guidelines further indicated that financial institutions should take appropriate measures to address risks arising from undertaking transactions through instructions that have been conveyed by customers over the internet, post or telephone.[46] The MAS Guidelines provide for specific measures such as:

(a) Telephone contact with the customer at a residential or business number that can be verified independently.

(b) Confirmation of the customer's address through an exchange of correspondence or other appropriate method.

(c) Subject to the customer's consent, telephone confirmation of the customer's employment status with the customer's employer's personnel department at a listed business number of the employer.

(d) Confirmation of the customer's salary details by requiring the presentation of recent bank statements from the bank.

(e) Certification of identification documents by lawyers or notary publics presented by the customers.

(f) Requiring the customer to make an initial deposit using a cheque drawn on the customer's personal account with a bank in Singapore (*i.e.* an FI regulated by MAS).

(g) Any other reliable verification checks adopted by the financial institution for non-face-to-face business.[47]

428. Holders of money-changer's or remittance business licences are prohibited from undertaking any business transaction without face-to-face contact with the customer except with the prior approval in writing of MAS which may attach such conditions and qualifications as it thinks fit (MAS Notice 3001 Para. 4.22). To date, MAS has not given such approval.

429. These provisions are fully reflected in MAS Notices to FIs and so are legally enforceable obligations. Furthermore, the MAS Guidelines to the Notices describe an appropriately wide-ranging set of measures that FIs could put in place effectively to manage the additional risk of doing business

---

45 MAS Notice 626 Para. 4.27; MAS Notice 824 Para. 30; MAS Notice SFA04-N02 Para. 4.27; MAS Notice FAA-N06 Para. 30; MAS Notice 314 Para. 4.28; MAS Guidelines 3001 Para. 30; MAS Notice TCA-N03 Para. 4.27.

46 MAS Notices on AML/CFT Para. 4.25 and 4.26; MAS Notice 314 Para. 4.26 and 4.27; MAS Guidelines 626, 1014, 824 Para.34; MAS Guidelines SFA04-N02 Para. 36; MAS Guidelines FAA-N06 Para.33; MAS Guidelines 314 Para.31; MAS Guidelines TCA-N03 Para. 30.

47 MAS Guidelines 626, 1014, 824 Para. 35; MAS Guidelines SFA04-N02 Para. 37; MAS Guidelines FAA-N06 Para. 34; MAS Guidelines 314 Para. 32; MAS Guidelines TCA-N03 Para. 31.

non-face to face with customers. Where non residents of Singapore are concerned, the FIs' head office, branches, subsidiaries or respondent banks in the prospective customer's home country are generally used to confirm identity.

Effectiveness

430. Overall, the provisions regarding non-face to face transactions are being effectively implemented. During their inspection, MAS examiners use the AML/CFT examination manual to check whether the financial institution being examined has implemented policies and procedures to mitigate the risks associated with accounts that are opened without face-to-face verification as well as when conducting on-going due diligence.

3.2.2 Recommendations and Comments

431. The MAS Notices covering AML/CFT issues broadly cover the FATF requirements for customer due diligence, including PEPs, correspondent banking, and non face-to-face business for nearly all financial institutions. However, certain basic CDD requirements (when CDD is required, required CDD measures, beneficial ownership) should be laid out in law or regulation. Nevertheless, the Notices create legal obligations with criminal sanctions apply for non-compliance. They are also treated as law or regulation by the financial sector, and this combined with the strong compliance culture in Singapore means that these measures are broadly observed and are being implemented effectively. Nevertheless, as required by the FATF standards, Singapore authorities should put the basic CDD obligations into law or regulation.

432. The fact that commodities futures brokers are currently not covered affects the ratings for Recommendations 5, 6 and 8. Singapore should move, as is currently planned, to cover these entities for AML/CFT purposes as quickly as possible.

433. With regard to Recommendation 5, Singapore should amend the AML/CFT notices to specify that reduced CDD measures are not allowed when there is a suspicion of ML/FT. MAS should also provide guidance about identifying possible linked transactions.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**LC**	• Certain requirements (when CDD takes place, required CDD measures, beneficial ownership, on-going due diligence) are contained in the Notices, which while they create legally enforceable obligations with criminal sanctions for non-compliance, are not in law or regulation as defined by the FATF. • It is not specified that simplified CDD provisions are not allowed whenever there is suspicion of ML/TF. • Non-bank FIs do not necessarily conduct sufficient risk assessments of new customers with a view to determining whether they are high risk customers to whom enhanced CDD measures should be applied. • Scope issues—commodity futures brokers will only be covered in 2008, and the implementation of CDD measures to moneylenders is too new to be assessed.
R.6	**LC**	• Scope issues—commodity futures brokers will only be covered in 2008.
R.7	**C**	• This Recommendation is fully observed.
R.8	**LC**	• Scope issues–commodity futures brokers will only be covered in 2008 by general requirements concerning non-face-to-face business, and the implementation of relevant measures to moneylenders is too new to be assessed.

3.3 Third Parties and Introduced Business (R.9)

3.3.1 Description and Analysis

434. Financial institutions (other than money changers, remittance businesses, and CIS trustees) are permitted to rely on intermediaries to perform some of the elements of the CDD process (other than ongoing monitoring of customers). Consequently, for the purposes of this section of the report (section 3.3), references to "financial institutions" does not include money changers, remittance businesses, CIS trustees and moneylenders.

435. Financial institutions may only rely upon an intermediary if the following requirements are met. First, the intermediary cannot be one which MAS has specifically precluded from being relied upon (MAS Notices on AML/CFT Para. 7.1(b)). No specific company or intermediary has ever been listed by the MAS as not to be relied upon – rather, a whole class, money services businesses – has been excluded.

436. The intermediary must be willing and able to provide without delay, and upon the financial institution's request, any relevant documentation that the financial institution requires or wants to obtain: MAS Notices on AML/CFT Para. 7.1(d). However, there is no requirement in the MAS Notices that FIs must immediately obtain from the intermediary CDD information on the introduced customer. MAS Notices on AML/CFT Para. 7.1(c) indicates that "the information that the financial institution would be required or would want to obtain and which is being obtained by the intermediary *may* be relayed to the financial institution by the intermediary without any delay" Discussions with fund managers confirmed that they have difficulty in obtaining the necessary information up front from independent financial advisor acting as intermediaries.

437. The financial institution must be satisfied that the intermediary is subject to and supervised for compliance with AML/CFT requirements consistent with the FATF standards, and has adequate measures in place to comply with those requirements (MAS Notices on AML/CFT Para. 7.1(a)). In the course of supervising for compliance with the above requirement, the MAS takes into consideration the FATF Mutual Evaluation Reports on countries, the FATF NCCT lists, FSAP reports, UNSC advisories and other publicly available sources of information such as commercial databases.

438. The MAS Notices explicitly state that, notwithstanding the reliance upon an intermediary, a financial institution shall remain responsible for the AML/CFT obligations (MAS Notices on AML/CFT Para. 7.4. This would include CDD obligations).

Effectiveness

439. The one major life insurance interviewed by the assessment team takes on approximately 90% of its new business either through its own sales force or through tied agents, with the remainder (a small, but growing, percentage) through financial advisers. The assessment team was assured that these financial advisers do indeed pass on all CDD information about policyholders to the insurance company immediately after take-on. This is required by the company, in order to be satisfied that it has the minimum CDD it requires on the policyholder for the business to proceed.

440. The situation is somewhat different where fund managers are concerned, because of the collective investment fund distribution model that exists in Singapore. Sales of these funds take place through a network of tied agents (who are, in effect, appointed representatives of the financial institutions for whom they work and sell only those institutions' products) and financial advisers who, while obliged by MAS to give prospective clients impartial advice, are nevertheless, in effect, "multiple tied agents" of a number of product providers. This means that the distributor, whether tied agent or financial adviser, is treated, for AML/CFT purposes, as the customer of the fund manager. The distributor maintains a consolidated omnibus account with the fund manager and deals directly with end-investors. The distributor is licensed by the MAS and required, under MAS AML/CFT Notices, to perform the necessary CDD measures on those end investors. In this distribution model, the distributor

processes fund subscription and redemption requests, via "bunched orders" through its omnibus account, sends out monthly statements, and handles any other requests made by end-investors. In these circumstances, it is clear that the tied agent or financial adviser, when acting as a distributor for a fund manager, is not acting as an introducer of business to the fund manager for the purposes of Recommendation 9. However, where the fund manager sells its funds directly to clients, or holds individual client accounts, that fund manager is responsible itself for performing required CDD measures on the clients. So, in a situation where law enforcement or the MAS wanted CDD information on a particular client, it would seek the information either from the fund manager or the distributor, depending on how the fund had originally been sold to the client. And there would be no difficulties about breach of customer confidentiality or data protection obligations.

3.3.2 Recommendations and Comments

441. The requirements in the MAS Notices broadly meet the FATF requirements with regard to introduced business. However, Singapore authorities should clarify that financial institutions must immediately obtain all the necessary CDD information up front on introduced customers. Singapore should also ensure that commodities futures brokers are made subject to requirements in relation to Recommendation 9 as quickly as possible.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**LC**	• No requirement that FIs should immediately obtain CDD information on introduced customers. • Scope issues–commodity futures brokers will only be covered in 2008.

3.4 Financial Institution Secrecy or Confidentiality (R.4)

3.4.1 Description and Analysis

442. Financial institution secrecy law is expressly lifted for the combating of money laundering and terrorist financing. For instance, there is a duty to report the suspicion of ML (s.39(1) CDSA) and it is expressly provided that such reporting will not be treated as a breach of any restriction upon disclosure imposed by law (including financial institution secrecy law) (s.39(6) CDSA). There is also a duty to report the suspicion of FT (s.8(1) TSOFA) and it is expressly provided that no criminal or civil proceeding (including any proceeding arising from breach of financial institution secrecy law) will lie against a person for terrorist financing reporting (s.8(5) TSOFA).

443. No rules or laws of financial institution secrecy inhibit the implementation of the FATF Recommendations. Singapore's authorities do share information with their foreign counterparts through formal and informal channels. Singapore is able to render assistance to foreign authorities for combating ML/FT under MACMA. Financial institution secrecy law is expressly lifted for the provision of such assistance. A financial institution has to produce the information requested by the foreign authority and is not excused from production on the basis that such production would be in breach of a legal obligation not to disclose it (including non-disclosure obligations under financial institution secrecy law) (s.23(3) MACMA).

444. Financial institutions are also required to share information with other financial institutions under MAS Notices to meet the requirements of Recommendations 7, 9 and Special Recommendation VII (MAS Notices on AML/CFT Para. 7 to Para. 9). Failure by the financial institutions to comply with these Notices is expressly made a criminal offence (s.27B MAS Act) and there is nothing in the Act that makes an exception on the basis of financial institution secrecy law.

Effectiveness

445. The MAS is able to share information with its counterparts abroad, both formally and informally. Formally, the MAS has over 20 MOUs in place internationally. And, informally, sharing of information has routinely taken place for many years, *e.g.* in relation to "fit and proper" checks. The basis of information sharing is that the MAS passes information to foreign regulatory bodies where, in the MAS's judgement, the foreign regulator has a need to know. A prime example of this is the MAS passing copies of its AML/CFT inspection reports to the regulator responsible for the parent company of FIs located in Singapore. The international protocol is that the foreign regulator is using the information for a regulatory purpose and that it does so confidentially.

3.4.2 Recommendations and Comments

446. This Recommendation is fully observed.

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**C**	This Recommendation is fully observed.

3.5 Record Keeping and Wire Transfer Rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10 (Record keeping)

447. Singapore addresses all of the substantive requirements of Recommendation 10; however, some aspects are implemented through MAS Notices, which are “other enforceable means” and not law or regulation, as is required by the FATF Recommendations. Also, there is a very narrow gap in scope which impacts the rating; commodities futures brokers are not subject to comprehensive record keeping obligations.

Maintaining transaction records

448. Sections 36 and 37 of the CDSA requires financial institutions to maintain all “financial transaction documents” for at least 5 years after the date on which the transaction takes place or the account is closed. The CDSA’s definition of “financial institutions" excludes licensed money-changers and remitters, moneylenders and commodities futures brokers. However, the Money-changing and Remittance Businesses Act (MCRBA) requires licensed money remitters and changers to keep complete records of all transactions for at least 5 years after the day on which the transaction takes place or the account is closed (s.16). Similar requirements apply in relation to moneylenders (“books of accounts relating to his business so as to exhibit and explain the financial position of his business”) (s.19(2)(a) Moneylenders Act).

449. The AML/CFT Notices also require financial institutions (other than moneylenders and commodities futures brokers) to retain records relating to a transaction, including any information needed to explain and reconstruct the transaction, for at least five years following the completion of the transaction.[48] It is not explicitly stated in the MAS Notices that the five year retention period for transaction records applies, irrespective of whether the relevant account or business relationship is ongoing or has been terminated. However, the MAS is confident that FIs would understand the

[48] MAS Notice 626, 1014 Para. 10.1 - 10.2; MAS Notice 824 Para. 9.1 - 9.2; MAS Notice SFA 04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 8.1 - 8.2; MAS Notice SFA13-N01 Para. 5.1 - 5.2.

obligation as applying to all transaction records, and the 5-year requirement is clearly stated in the CDSA, in any event.

450. Financial institutions (other than moneylenders and commodities futures brokers) are further required to retain records pertaining to a matter under investigation or which has been the subject of an STR for such longer period as requested by MAS, STRO and other relevant authorities.[49] Financial institutions are required to prepare, maintain and retain documentation on all its business relations and transactions with its customers such that any transaction undertaken can be reconstructed so as to provide evidence for the prosecution of criminal activity, if necessary.[50]

Maintaining identification data, account files, and business correspondence

451. According to Recommendation 10, financial institutions should be required by law or regulation to maintain records of identification data, account files and business correspondence for at least five years following termination of an account or business relationship. The CDSA contains such requirements in relation to identification data for financial institutions other than money changers and remitters, moneylenders and commodities futures brokers. The CDSA's definition of the "financial transaction documents" that must be maintained includes, but is not limited to, records of customer identification. Although there is no specific mention of "account files", the documents relating to account opening/closing, account operation, wire transfers, opening or use of a safety deposit box and loan applications must also be kept, and would seem to capture that concept. Money changers and remitters do not maintain customer "accounts" per se, as they deal with occasional customers. Moneylenders are required to maintain account records for at least 5 years according to section 19 of the Moneylenders Act.

452. "Business correspondence" is not specifically mentioned in either the CDSA or the corresponding MCRBA requirements. These requirements are implemented through the MAS Notices that are "other enforceable means" with criminal penalties for non-compliance, and do not apply to commodities futures brokers. This impacts the rating.

453. In accordance with s.16 of the MCRBA, all holders of money changer or remittance business licences are required to keep complete records of all the transactions in such books, accounts, records and registers as the Authority may specify from time to time. By implication, the requirement for the licensees to maintain complete records of all transactions would include any correspondences with its customers, agents, etc.

454. In addition, MAS Notice 3002, which is issued pursuant to sections 16 and 30 of the MCRBA, requires all licensees to maintain complete records of all transactions in registers and copies of identification documents of the customer or person acting on behalf of the customer for money-changing transactions of SGD 5,000 and above and for every remittance transaction. Therefore, licensees are required under section 16 read with para. 2 of MAS Notice 3002 to maintain identification data.

455. Section 19(2)(c) of the Moneylenders Act provides for the retention of "such other documents as may be prescribed" for not less than five years. Under Rule 12(3) of the Moneylenders Rules, moneylenders are required to keep a copy of the memorandum of loan for at least five years.

456. Requirements to maintain records of business correspondence are expanded upon the MAS Notices, but not in law or regulation as is required by the FATF standards. The MAS Notices require documents containing customer identification information, as well as those relating to the establishment of the business relation, account files and business correspondences to be kept for a period of at least five

[49] MAS Notice 626, 1014 Para. 10.4; MAS Notice 824 Para. 9.4; MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 8.4; MAS Notice SFA13-N01 Para. 5.4.

[50] MAS Notice 626, 1014 Para. 10.1 (b); MAS Notice 824 Para. 9.1 (b); MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 8.1 (b); MAS Notice SFA 13-N01 Para. 5.1 (b).

years following the termination of the business relation. These requirements apply to records relating to all customers (*i.e.* both domestic and international).[51]

Ensuring records are available to competent authorities

457. Section 37 of the CDSA requires documents be stored in a manner that makes retrieval of the documents reasonably practicable. Section 16 of the MCRBA requires money changers and remittance agents to make records available to their supervisor when requested to do so in writing. In addition, under the MAS Notices, financial institutions are required to ensure that it can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities for information.[52] The Registrar of Moneylenders has the powers under Section 10A of the Moneylenders Act to require moneylenders to provide him with documents or information required. He also has powers under section 19(5) of the Moneylenders Act to inspect the books of accounts of moneylenders. However, there are no corresponding requirements applicable to commodities futures brokers.

Effectiveness

458. Overall, the record keeping requirements are being implemented effectively. During on-site inspections, MAS examiners review the record keeping policies and procedures that are in place. MAS examiners will also ascertain that the information kept by financial institutions creates a satisfactory audit trail of suspicious ML transactions and sample test customer files to ensure that financial institutions comply with the requirements under the Notices. Sample testing is done on customer files for existing customers as well as customers who have ceased business relations with the financial institution to ascertain if the financial institution has fulfilled the record keeping requirements.

Special Recommendation VII (Wire transfers)

459. For the purposes of discussing Special Recommendation VII in this section, all references to financial institutions are limited to banks, merchant banks, finance companies and holders of a remittance business licences. They are the only financial institutions in Singapore authorised to carry out wire transfers; therefore the fact that obligations for SR.VII do not apply to other financial institutions is not relevant.

460. For both cross-border and domestic wire transfers exceeding SGD 2 000 (approximately EUR 1 000) in value, the ordering financial institution (*i.e.* the financial institution that is sending the wire transfer on behalf of the customer) is required to identify and verify the identity of the customer who is the originator of the transaction by obtaining:

(a) The name of the originator.

(b) The originator's account number (or unique reference number).

(c) The originator's address (or unique identification number, or date and place of birth).

(MAS Notice 626, 1014 Paras 9.4 and 9.5; MAS Notice 824 Para 8.4 and 8.5; MAS Notice 3001 Para. 7.4 and 7.5).

[51] MAS Notice 626, 1014 Para. 10.1 - 10.2; MAS Notice 824 Para. 9.1 - 9.2; MAS Notice SFA 04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 8.1 - 8.2; MAS Notice SFA13-N01 Para. 5.1 - 5.2.

[52] MAS Notice 626, 1014 Para. 10.1 (d); MAS Notice 824 Para. 9.1 (d); MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 8.1 (d); MAS Notice SFA 13-N01 Para. 5.1 (d).

461. The requirements under Recommendation 5 relating to the verification of the originator's identity (as detailed in Para 4 of MAS Notice 626, MAS Notice 824, MAS Notice 1014 and MAS Notice 3001) apply to ordering financial institutions before they effect wire transfers, regardless of the amount of the transfer involved.[53]

462. For all cross-border wire transfers exceeding SGD 2 000 (approximately EUR 1 000) in value, the ordering financial institution must include the full originator information (as listed above) with the wire transfer (or payment instruction that accompanies the wire transfer).

463. Ordering financial institutions are required to ensure that these requirements are adequately communicated and explained to their customers and that they have the necessary customer consent to include such information in the wire transfer or payment instruction.[54] Customer consent to include originator information must be obtained for data protection reasons and the order form to be completed by the transferor, before payment is made, incorporates a box that must be ticked by the transferor to indicate that he has given consent. If he/she is unwilling to tick the box, the payment is simply not made. Batching of individual wire transfers does not appear to be an issue in Singapore and is therefore not covered in the Notice.

464. Banks, merchant banks and finance companies do not batch individual wire transfers. Certain remittance licensees would collate several transactions from customers before sending these to the banks for transfer of the funds to the beneficiaries. This is done mainly for the purpose of convenience due to the voluminous number of transactions handled daily.

465. To address the higher risks posed by the remittance licensees, banks would assess their AML/CFT control framework by conducting visits to the remittance licensees' premises. The banks also have a practice to query the remittance licensees on the identities of the beneficiaries and ordering parties for large and unusual transactions.

466. For a domestic wire transfer exceeding SGD 2 000 (approximately EUR 1 000) in value, where the ordering financial institution is not able to obtain the full originator information, only the originator's account number (or unique reference number) needs to be included in the wire transfer (or accompanying payment instruction). However, the ordering financial institution must be in a position to make the remaining originator information available within three working days of a request being made by the beneficiary financial institution (*i.e.* the financial institution that received the wire transfer on behalf of a customer). Additionally, all financial institutions (including ordering financial institutions) are required to satisfy an enquiry from competent authorities for information within any time period specified by the authorities.[55] Law enforcement authorities can compel the immediate production of originator information in the same way as for any other information if it is desirable for any investigation or inquiry under the CPC, including those relating to ML/FT (s.58 CPC).

467. When passing on a wire transfer or payment instruction, intermediary financial institutions are required to maintain with the wire transfer all of the required originator information.[56]

468. There is no explicit provision in the Notices covering the need, where technical limitations prevent full originator information accompanying a transfer, for a record to be kept for 5 years of all the information that was actually received from the ordering FI. However, there is a general requirement on all financial institutions to keep records on all its business relations and transactions with its customers,

---

53 MAS Notice 626, 1014 Para. 9.3; MAS Notice 824 Para. 8.3. MAS Notice 3001 Para 7.3.

54 MAS Notice 626, 1014 Para. 9.4 and Para. 9.5; MAS Notice 824 Para. 8.4 and Para. 8.5; MAS Notice 3001 Para. 7.4 and Para. 7.5.

55 MAS Notice 626, 1014 Para. 9.5(b) and Para. 10.1(d); MAS Notice 3001 Para. 7.5(b) and Para. 8.1(d); MAS Notice 824 Para. 8.5(b) and Para. 9.1(d).

56 MAS Notice 626, 1014 Para. 9.7; MAS Notice 824 Para. 8.7; MAS Notice 3001 Para. 7.7.

the intermediary institution is also required to keep records on all the information received from the ordering financial institution for at least 5 years following the completion of the relevant wire transfer transaction.[57]

469. Beneficiary financial institutions are required to implement appropriate internal risk-based policies, procedures and controls for identifying and handling in-coming wire transfers which are not accompanied by complete originator information. The risk-based procedures should include, but are not limited to, requesting for the missing originator information from the ordering bank. Beneficiary financial institutions are advised to consider filing the necessary suspicious transaction report with STRO if the ordering bank is unwilling to provide the missing information. They are also advised to consider not accepting in-coming wire transfers from or terminating business relations with overseas ordering financial institutions that, to their knowledge, are required to provide originator information but fail to do so. The MAS indicated that it recognised that not all countries have implemented Special Recommendation VII yet, hence the guidance indicates that FIs should take into account any requirements that may be imposed on the overseas ordering bank, either by law or as a regulatory measure, in respect of cross-border wire transfers.[58]

470. MAS monitors compliance with requirements on wire transfers under MAS Notices and Guidelines through on-site AML/CFT inspections. In the course of on-site inspection, MAS reviews the financial institutions' risk management and control systems for wire transfers to ensure that they comply with the requirements under the MAS Notices. It is emphasised that financial institutions should know the identity and business of the customer on whose behalf they approve funds transfers to minimise the possibility of money laundering. As funds may be aggregated from different sources and moved through accounts with different financial institutions to disguise their origins, MAS examiners also check that proper monitoring procedures to detect and review any unusual funds transfer activities are properly instituted by the financial institutions and that effective procedures on the escalation and reporting of suspicious transactions are in place. To ensure complete record keeping and effective monitoring of past compliance conduct of the financial institutions, MAS maintains a central database of all inspection findings on AML/CFT.

471. As with other violations of the Notices, persons who fail to comply shall be liable on conviction to a fine not exceeding SGD 1 000 000 and, in the case of a continuing offence, to a further fine of SGD 100 000 for every day during which the offence continues after conviction (These fines were raised from SGD 100 000 and SGD 10 000 respectively pursuant to amendments to the MAS Act which entered into force on 1 November 2007). The MAS informed the assessment team that breaches of wire transfer obligations set out in the Notices would also be subject to administrative sanctions in the same way as any other breach of MAS requirements by FIs.

Effectiveness

472. There are global concerns (*i.e.* not Singapore-specific) about technical issues that may prevent full originator information from being transmitted, as the assessment team was informed by one of the banks that the biggest practical problem for FIs in implementing Special Recommendation VII is the lack of sufficient space in SWIFT message fields, for both originators and beneficiaries, to include all the information that compliance with the Notice requires.

473. The banks indicated that they had some concerns, qua beneficiary FI, about receiving inadequate originator information. If the ordering bank was located in a FATF country, the missing information was easily obtained upon request. But where the ordering bank was in a higher risk country, missing

[57] MAS Notice 626, 1014 Para. 10.1 and Para. 10.2(b); MAS Notice 3001 Para. 8.1 and Para. 8.2; MAS 824 Para. 9.1 and Para. 9.2(b).

[58] MAS Notice 626, 1014 Para. 9.6; MAS Guidelines 626, 1014, 824 Para. 57 – Para. 58; MAS Guidelines 824 Para. 8.6; MAS Guidelines 3001 Para. 7.6; MAS Guidelines 3001 Para. 40 – Para.41.

information was unobtainable – and the Singapore bank would not accept payments in those circumstances.

474. Singapore does not maintain statistics concerning the volume of international wire transfers, as is required by Recommendation 32.

Recommendations and Comments

475. Record keeping requirements are generally comprehensive and are generally observed; however, the requirements for financial institutions to maintain business correspondence, and the requirement for money exchange and remittance businesses to maintain identification data should be laid out in law or regulation. Comprehensive record keeping provisions should also be applied to commodities futures traders.

476. The MAS Notices broadly implement the requirements for SR.VII. However, the Notices should specify that, where technical limitations prevent the full originator information accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

477. Singapore should maintain statistics concerning the volume of international wire transfers.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• The requirements to maintain business correspondence are set out in other enforceable means, not law or regulation. • Commodities futures brokers will only be covered in 2008.
SR.VII	**LC**	• No explicit provision for record keeping where technical limitations prevent full originator information accompanying a cross-border transfer.

Unusual, Suspicious and other Transactions

3.6 Monitoring of Transactions and Relationships (R.11 & 21)

Recommendation 11 (Unusual transactions)

3.6.1 Description and Analysis

478. Financial institutions are required to pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose (MAS Notices on AML/CFT Para. 4.22). Examples of suspicious transactions are set out in Appendix II to the MAS Guidelines, which are not intended to be exhaustive. The examples are red-flag indicators of AML/CFT and if any similar or other transactions are identified, financial institutions should make further enquiries on the customers' activities/business and into the source of funds where necessary.

479. MAS Notices require financial institutions to inquire into the background and purpose of all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and document their findings with a view to making this information available to the relevant competent authorities should the need arise: MAS Notices on AML/CFT Para. 4.23.

480. Financial institutions are required to prepare, maintain and retain documentation on all of their business relations and transactions. This includes documentation on the internal findings and analysis of the financial institution relating to complex or unusually large transactions or unusual patterns of

transactions that have no apparent or visible economic or lawful purpose. These documents are required to be made available to the competent authorities and auditors for at least five years.[59]

Effectiveness

481. MAS determines, through onsite examinations, if a financial institution monitors on an ongoing basis its business relations with customers, and scrutinises transactions undertaken to ensure that the transactions are consistent with the institution's knowledge of the customer, its business and risk profile and where appropriate, the source of funds. Examiners determine, for example, (1) if the financial institution has well-defined guidelines and procedures in place for investigating, reporting and acting on suspicious transactions; (2) if the institution's channels for reporting suspicious transactions have been clearly specified in writing and communicated to all personnel. They also review the accuracy, timeliness and usefulness of management reports prepared for the surveillance of possible ML/FT activities, and the systems in place to aggregate and monitor significant balances and activity in customer accounts on a consolidated basis.

482. Financial institutions that the onsite team met with explained that they have established monitoring systems and procedures to identify unusual and potentially suspicious customer behaviour. Their automated surveillance systems with pre-determined rules that flag transactions which match certain conditions set under local money laundering rules allow the monitoring staff to review flagged transactions in a timely fashion, and even if they have determined that there are no grounds for suspicion, they have kept records of the reasons for dropping the cases as suspicious ones to be reported to the STRO.

483. As the requirements in relation to moneylenders (Rule 7 of the Moneylending Rules) were only recently enacted, it is not yet possible to assess effectiveness.

Recommendation 21 (Countries that insufficiently apply the FATF Recommendations)

484. Financial institutions are further required to give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the financial institutions for themselves or notified to financial institutions generally by MAS or other foreign regulatory authorities (MAS Notices on AML/CFT Para. 6.3 – Para. 6.4).

485. Since the FATF issued its Non-Cooperative Countries and Territories (NCCT) List in 2000, MAS has issued circulars to financial institutions notifying them of which jurisdictions had been identified as NCCTs or subjected to FATF-imposed countermeasures, and informing them of the need to pay special attention to transactions related to such jurisdictions due to the possibility of heightened money laundering risks. Since 1995, MAS has been using MASNET to disseminate circulars to the financial institutions electronically. For financial institutions that do not subscribe to MASNET, circulars are sent to them via post. Between 2000 and 2006, 5 circulars on the NCCT list were issued.

486. MAS has also issued circulars informing financial institutions of blacklisted persons and entities with whom business relations are strictly prohibited such as the 1267 Committee. MAS uses its public website to inform financial institutions of the updates on the UNSCR lists and the MAS (ATM) Regulation on the freezing of assets of persons from countries listed by the United Nations, as and when they occur. Financial institutions subscribe to the MAS email system which alerts them to updates on the MAS website. In addition, financial institutions are encouraged to refer to other sources of information to identify higher risk countries or jurisdictions.

[59] MAS Notice 626, 1014 Para. 10.1 – Para. 10.4; MAS Notice 824, 3001 Para. 8.1 – Para. 8.4; MAS Notice SFA04-N02, FAA-N06, 314, TCA-N03 Para. 8.1 – Para. 8.4; MAS Notice SFA 13-N01 Para 5.1 – Para. 5.4.

487. If a transaction involving such a country or high-risk person is found to have no apparent or visible economic or lawful purpose, the financial institution is required to inquire into the transaction's background and purpose. The findings are to be documented with a view of making this information available to MAS, STRO and other relevant law enforcement agencies, should the need arise.[60]

488. MAS has not exercised powers to apply such counter-measures as exemplified in the FATF standards by means of enforceable regulations to require financial institutions to apply stringent or additional AML/CFT measures beyond normal obligations (set out in the MAS Notices described earlier) in relation to transactions with, or financial institutions from, countries that continue not to apply or insufficiently apply the FATF Recommendations.

489. In line with the FATF's decision to impose countermeasures on Nauru, Ukraine and Myanmar, MAS issued circulars to advise the financial institutions under its purview to be aware of ML risks in these countries and to give special attention to transactions with persons or entities from the countries. However, these circulars have no enforceability like the MAS Notices. The circulars provide that :

(a) Financial institutions are reminded of customer identification requirements specified in the Notice on Prevention of Money Laundering and should ensure that identification of beneficial owners is performed before the commencement of new business relationships with persons or entities operating from these countries.

(b) Financial institutions should monitor account activities of customers from these countries for deviation from expected activities based on known information about such customers. Where there are grounds for suspicion, clarification should be sought from customers and if it is unsatisfactory, institutions should make a suspicious transaction report.

490. In assessing new applications for licence in Singapore, MAS assesses the home countries' compliance with the FATF standards based on FATF and FSAP reports, and requires the financial institution to furnish information on compliance procedures, including whether it has been sanctioned for AML/CFT breaches.

Effectiveness

491. Financial institutions interviewed indicated that they have been taking into account the risk associated with the geographical connections of the customer, such as the jurisdiction in which the customer's operations are based or the jurisdiction of origin or incorporation. Country risk assessment focuses on customers and transactions that require additional due diligence and monitoring for their susceptibility to ML/FT risk. It ranks countries around the world as high, moderate or low risk based on such factors as the degree to which corruption is perceived to exist among public officials and politicians as measured by the Transparency International Corruption Perceptions Index and the presence of detrimental rules and practices which obstruct international co-operation against money laundering as identified as NCCTs by the FATF.

3.6.2 Recommendations and Comments

492. Financial institutions are legally required through MAS Notices or the Moneylending Rules to pay special attention to unusual transactions and transactions from higher risk countries, and to examine and document their backgrounds and purposes. Commodities futures brokers should be made subject to requirements in relation to Recommendations 11 and 21. As the measures applicable to moneylenders is very recent, it is recommended that the Ministry of Law make sure that these institutions effectively comply with the new regulations through the same level of offsite and onsite oversight regimes that currently apply to the other financial institutions.

[60] MAS Notices on AML/CFT Para. 4.22 – 4.23; MAS Notice 3001 Para. 4.20 – 4.21.

493. Singapore authorities should exercise enforceable powers to require financial institutions to apply additional AML/CFT counter-measures beyond normal obligations (set out in the MAS Notices described earlier) in relation to transactions with, or financial institutions from, countries that continue not to apply or insufficiently apply the FATF Recommendations.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	**LC**	• Commodities futures brokers will only be covered in 2008. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
R.21	**LC**	• No enforceable powers have been exercised to require financial institutions to apply stringent or additional AML/CFT counter-measures against those countries which continue not to apply or insufficiently apply the FATF Recommendations. • Commodities futures brokers will only be covered in 2008. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.

3.7 Suspicious Transactions and other Reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis

Recommendation 13 and Special Recommendation IV (Suspicious transaction reporting)

494. Section 39 of the CDSA requires that any person who, in the course of his/her professional or business duties, knows or has reasonable grounds to suspect that any property may represent the proceeds of drug trafficking or criminal conduct (as defined in section 2(1) of the CDSA), or was used or is intended to be used in connection with drug trafficking or criminal conduct (which includes ML/FT) is obliged to disclose the knowledge or suspicion to an STRO officer (as per amendments to the CDSA, effective 1 November 2007. Previously, the CDSA referred more generally to reporting to "an authorised officer.") "Criminal conduct" is defined, among other things, as to include a total of 335 "serious offences" listed in the First and Second Schedule of the CDSA as at 14 November 2007. The scope of the predicate offences, however, does not satisfy all the requirements set under the international standards as discussed in Section 2.1.

495. MAS Notices further clarify that financial institutions, while keeping in mind the provision in the CDSA and the TSOFA that provide for the reporting to the competent authorities of transactions suspected of being connected with ML/FT, must submit their reports on suspicious transactions to the STRO and extend a copy to MAS for information (para. 11.2 of Notice 626 for banks, with similar wording in the other notices). MAS Guidelines define money laundering referred to in the MAS Notices broadly as a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. This MAS requirement, coupled with the broader ML definition, seems wide enough to fill the minor gap in the scope of predicate offences and encompasses the necessary elements recommended by the FATF standards. It should be noted again, however, that the MAS Notices are not considered law or regulation as required by FATF.

496. Financial institutions are required to implement appropriate internal policies, procedures and controls in relation to the reporting requirement. This includes establishing a single reference point within the organisation, to whom all staff are required to promptly refer all transactions suspected of being connected with ML/TF, for possible referral to the STRO (*i.e.* through the filing of an STR).

Financial institutions are also required to keep records of all suspicious transactions which they have referred to STRO, including any internal findings and analysis performed on these transactions.[61]

Reporting suspected terrorist financing

497. Since terrorism financing (i.e. offences under Section 3, 4, 5 and 6 of TSOFA) is listed as a serious offence in the CDSA, the requirement under section 39 for anyone who knows or has reasonable grounds to suspect that any property may represent the proceeds of, was used in connection with, or is intended to be used in connection with terrorism financing is required to lodge a STR. Terrorism financing in this context is defined under the TSOFA as (1) providing or collecting property for terrorist acts (s.3); (2) provision of property and services for terrorist purposes (s.4); (3) use or possession of property for terrorist purposes (s.5); and (4) dealing with property of terrorists (s.6).

498. In addition, TSOFA imposes duties upon all persons in Singapore (s.10) and Singapore citizens outside of Singapore (s.8) to disclose to a police officer any information regarding possession, custody or control of terrorist property, on a terrorist transaction in respect of any property belonging to terrorist or terrorist entity or about acts of terrorism financing.

499. Regulation 9 of the MAS (ATM) Regulations 2002 imposes upon financial institutions the duty to disclose to MAS if it has possession, custody or control of any property, belonging to any terrorist or any entity owned or controlled by any terrorist. Every financial institution also has a duty to disclose any information about any transaction or proposed transaction in respect of any property belonging to any terrorist or any entity owned or controlled by any terrorist.

Attempted transactions and those related to tax matters

500. As described above, section 39 of the CDSA requires any person to disclose "knowledge or suspicion" to the police authorities. The scope of what must be disclosed to STRO under this legal requirement (*i.e.* "knowledge or suspicion") seems broad enough to cover all suspicious transactions (including those that may be related to ML/FT), regardless of amount, that are identified by financial institutions. Whether this scope includes attempted transactions or not is clarified in the MAS Notices, which explicitly require financial institutions to submit reports on suspicious transactions (including attempted transactions) to STRO and extend a copy to the MAS for information.[62]

501. Where the conditions under section 39 of the CDSA or sections 8 and 10 of the TSOFA are met, suspicious transaction reporting is required, regardless of whether the transaction involves tax matters. MAS Notices do not provide for any exception of STR reporting requirement by reason of tax related matters.

Additional elements

502. Financial institutions are required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of criminal acts. The scope of criminal conduct, whether in Singapore or elsewhere, is defined in section 1 of the CDSA.

Recommendation 14 (Safe harbour and tipping off)

503. A person (including an employee of a financial institution) is not in breach of any legal restriction on the disclosure of information if he/she discloses to a police officer the knowledge or suspicion that property is proceeds of crime (s.39(6) CDSA). Likewise, a person making such a

[61] MAS Notice 626, 1014 Para. 11.1; MAS Notice 824 Para. 10.1; MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 9.1; MAS Notice SFA13-N01 Para. 6.1.

[62] MAS Notice 626, 1014 Para. 11.2; MAS Notice 824 Para 10.2; MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para 9.2; MAS Notice SFA13-N01 Para 6.2.

disclosure is not liable for any loss arising out of the disclosure or any act or omission in consequence of the disclosure.

504. For reporting of incidents relating to the financing of terrorism, sections 8(5) (duty to disclose possession of terrorist property or transactions relating to it), 9(3) (duty to determine possession of terrorist property on a continuous basis) and 10(3) (duty to disclose information to prevent FT offence) of TSOFA provide that no criminal or civil proceedings shall lie against a person for a disclosure made in good faith.

505. Tipping off is an offence under the CDSA. It is an offence for any person with knowledge that an investigation under the CDSA (which includes all predicate offences, including terrorism financing) is taking place or is about to take place to make any disclosure likely to prejudice the investigation (s.48(1) CDSA). Reference to this provision under CDSA is also spelled out in MAS Notices.[63]

506. Section 48 (2) of the CDSA, on the other hand, provides that any person who (a) knows or has reasonable grounds to suspect that a disclosure *has been made* to an authorised officer under this Act (referred to in this section as the disclosure); and (b) discloses to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following the disclosure, shall be guilty of an offence. This legal provision refers only to those cases where a STR or related information has been already reported to the FIU, and does not appear to encompass cases where a transaction is still taking place, or an STR/related information is in the process of being reported to the FIU.[64]

Recommendation 25 (only feedback and guidance related to STRs)

507. STRO (the FIU) and MAS provide reporting entities with a significant amount of feedback concerning the STR reporting obligation.

508. **Publications:** To date, STRO has published four issues of "Reports from STRO" which is a newsletter that provides important updates on AML/CFT issues (*e.g.* common STR typologies in Singapore, domestic and international trends affecting Singapore, basic statistics on the STR regime, common indicators of a suspicious transaction and sanitised STR case studies (see section 2.5 for a full description). The CAD/STRO Annual Report also contains information on the STR reporting regime.

509. **Feedback forms:** STRO has designed and circulated feedback forms to STR reporting entities. As part of the specific feedback to the STR reporting entities, STRO informs them of the analysis outcome on the STR lodged and (in some cases) the outcome of investigations relating to the STR matter. STRO may also further advise the STR reporting entities on potential weaknesses in their financial products or system that could be abused by the criminals. In some cases where an STR has led to the discovery of a major criminal offence, FID has sent letters of appreciation to the reporting entity.

510. **Outreach:** Between 2004 and 14 November 2007, STRO has conducted 31 outreach sessions to the financial sector, during which case studies that arose from STRs were highlighted. During such events, recent trends and examples of good STRs are shared with participants. These events also include close door discussions with the senior management of the financial institution. STRO reports that such sessions have been warmly received, and have led to more candid exchanges and enhanced the quality and quantity of STRs received. STRO also advises reporting institutions of the number of STRs received and the amount of money seized by FID/CAD to date.

---

63 MAS Notice 626, 1014 Para. 11.1; MAS Notice 824 Para. 10.1; MAS Notice SFA04-N02, FAA-N06, 314, 3001, TCA-N03 Para. 9.1; MAS Notice SFA13-N01.

64 This deficiency was not identified in previous FATF mutual evaluation reports of countries with similarly worded tipping off provisions.

511. **STRO's hotline:** During STRO's outreach sessions, organisations and individuals are encouraged to contact STRO via this hotline to discuss important "live" or highly urgent cases. The hotline is used at an average of twice a week over the last few years. The hotline is manned by the Head of STRO with a view to ensuring that timely advice is given at the highest level within STRO for urgent matters. Common examples of hotline queries relate to large withdrawals by bank customers which appear to be under suspicious circumstances, and whether specific scenarios are sufficiently "suspicious" to trigger an STR.

512. **STRO's webpage:** The information provided on the STRO webpage includes information pertaining to STRO's AML/CFT Handbook, frequently asked questions (FAQs) relating to the reporting and detection of STRs, and details of key AML/CFT related events organised by STRO and FID. From time to time, sanitised cases, updated information on typologies and general feedback by STRO to the industry or members of the public is published.

513. **STROLLS Pilot Project:** The Suspicious Transaction Report OnLine Lodging System (STROLLS) which allows users to lodge STRs securely via internet also has a bulletin which can be assessed by STROLLS members which provides updates relating to key indicators of suspicious transactions, legislation and STRO in general, among others. See section 2.5 of this report for more information on STROLLS.

514. **MAS guidelines:** The Guidelines to the MAS Notices provide further guidance to the financial institutions on suspicious transaction reporting. For instance, financial institutions are to ensure that the internal process for evaluating whether a matter should be referred to STRO via an STR are completed without delay and not exceeding 15 working days of the case being referred by the relevant staff of the financial institution, unless the circumstances are exceptional or extraordinary. The Guidelines also provide examples of suspicious transactions.[65]

Recommendation 19 (Other types of reporting)

515. Prior to enacting the CDSA, Singapore deliberated on the pros and cons of requiring financial institutions to report all transactions above a fixed threshold to a national central agency. After due consideration, Singapore decided not to adopt such a system for the following reasons:

(a) Inefficient use of financial institutions' resources to track and report all transactions above a fixed threshold when most of such transactions are known to be attributable to legitimate businesses.

(b) The maintenance and proper analysis of such a huge data base of transactions would require significant resources from the national central agency. From an enforcement perspective, this is not an effective approach to sieve out suspicious transactions for follow up actions.

(c) Financial institutions in Singapore have been advised that a cash transaction of SGD 20 000 (approximately EUR 10 000) is sufficiently large to raise a suspicion, especially in cases where the occasional customers have not established business relationships with the financial institutions (*e.g.* money changers). In effect, cash transactions above this threshold are in all likelihood reported to STRO when the financial institutions do not have any information about the source and purpose of such transactions.

516. Singapore authorities reported that, during the FSAP Evaluation in 2003/2004, the AML Inter-Agency Committee deliberated again on the pros and cons of routine threshold reporting. Singapore reviewed and affirmed its decision not to require financial institutions to report transactions above a fixed threshold taking into consideration the efficiency and effectiveness of such a measure. Singapore

[65] MAS Guidelines 626, 1014, 824, SFA04-N02 Para. 59 – 65; MAS Guidelines FAA-N06 Para. 55 – 61; MAS Guidelines 314 Para. 53 – 59; MAS Guidelines 3001 Para. 42 – 48; MAS Guidelines TCA-N03 Para. 47 – 53; MAS Guidelines SFA13-N01 Para. 22 – 28.

views it as more effective for financial institutions to build up their alertness and sensitivity to ascertain whether a transaction is indeed suspicious regardless of the amount involved and file suspicious transactions to STRO.

Statistics and effectiveness

517. The breakdown of the STRs received from the various financial institutions and other reporting entities are as follows.

Breakdown of Suspicious Transaction Reports Received

	2004	2005	2006	2007 (as at 14 Nov.)
Banks	1 074	1 243	1 712	2 063
Insurance Companies	543	590	911	2 964
Money Changing and Remittance Agents	32	107	195	111
Capital Markets Intermediaries	24	60	350	1 039
Finance Companies	7	29	56	87
Government Agencies	57	25	26	30
Others (including individuals)	37	21	35	62
TOTAL	**1 772**	**2 075**	**3 285**	**6 356**

518. The number of STRs received by STRO has steadily increased since 2004. In particular, there has been a significant increase in the number of STRs being received from the financial sector – particularly from the capital markets industry and the insurance sector. All of the financial institutions met with during the on-site visit showed a good understanding of the reporting obligation. Feedback from STRO suggests that the quality of STRs is consistently high, and the reporting regime is not burdened by systematic defensive filing.

519. MAS reviews, through on-site examinations, whether systems and risk parameters that the financial institution uses in reporting suspicious activities are effective and appropriate within the context of the institution's business. Examiners assess, for instance, if the financial institution has established limits for a particular class or category of accounts and investigated transactions that exceed them or performed periodic analysis to identify transactions that are inconsistent with the client profile. They also ascertain, for all suspicious cases, if the financial institution has submitted a STR and, if not, whether it has documented the basis for its determination of whether the case warrants filing. They further ascertain if the financial institution has maintained a complete file of all transactions that have been brought to the attention of its AML/CFT compliance officer or unit, including transactions that are not reported to STRO.

520. Financial institutions that the assessment team visited indicated that they have been implementing a process to identify, track, escalate and report unusual activity to senior management in a timely manner to determine if there are reasonable grounds for suspicion to file an STR or if they should gather more information. In the process, if they have decided not to file a STR, they carry out procedures to document their findings and to impose other measures including enhanced monitoring or account closure to mitigate risk. They have also managed a process for responding to law enforcement requests and for investigating the customer activity.

521. The industry-specific guidance notes developed and issued by MAS with a lot of specific technical inputs from STRO have been well accepted and put to practical use by the financial industry. MAS has been in the best position to understand the risks involved in the respective financial businesses under its supervision. STRO has also been providing the reporting industry with effective indicators on the type of suspicious transactions to be reported. These joint efforts have produced notable results in the enhanced quality and increased number of STRs received by STRO for the last several years.

3.7.2 Recommendations and Comments

522. The reporting of suspicious transactions is made mandatory for all persons, including all financial institutions, under the CDSA. Except for commodities futures brokers, the MAS Notices also impose such reporting requirement on financial institutions and ensure their compliance through onsite and offsite supervision. It is recommended that commodities futures brokers be also subject to the same regulatory requirement and supervision regime. Additionally, Singapore should broaden the range of offences to include human trafficking comprehensively, so as to ensure that the scope of the predicate offences for STR reporting is sufficient (see section 2.1 for a full discussion of this issue). Finally, certain aspects of the reporting requirements (reporting to STRO, attempted transactions) should be put into law or regulation.

523. It is recommended that the CDSA tipping-off provisions be expanded to include not only those cases where a STR or related information has been reported but also is in the process of being reported to the FIU.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**LC**	• The scope of the predicate offences for STR reporting does not satisfy all the FATF standards. • Certain clarifications of the law (reporting to STRO, attempted transaction) are covered in "other enforceable means" but not in law or regulation.
R.14	**LC**	• The scope of the tipping-off provision does not include a case where an STR is in the process of being reported to the FIU.
R.19	**C**	• This Recommendation is fully observed.
R.25	**LC**	• *(This is a composite rating and does not derive from the issues covered here.)*
SR.IV	**C**	• This Recommendation is fully observed.

Internal controls and other measures

3.8 Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22)

Recommendation 15

3.8.1 Description and Analysis

524. MAS Notices require financial institutions to develop and implement internal AML/CFT policies, procedures and controls, and to communicate them to their employees. The policies, procedures and controls should include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.[66]

525. MAS Notices require financial institutions to develop appropriate compliance management arrangements, including at a minimum, the appointment of a compliance officer who is at the management level and who is responsible for AML/CFT matters.[67] Guidance on the responsibilities of

[66] MAS Notice 626 Para. 12.1 – 12.2; MAS Notice 1014 Para. 12.1 – 12.2; MAS Notice 824 Para. 11.1 – 11.2; MAS Notice SFA04-N02 Para. 10.1 – 10.2; MAS Notice FAA-N06 Para. 10.1 – 10.2; MAS Notice 314 Para. 10.1 – 10.2; MAS Notice 3001 Para. 10.1 - 10.2; MAS Notice TCA-N03 Para. 10.1 – 10.2; MAS Notice SFA13-N01 Para. 7.1 - 7.2.

[67] MAS Notice 626 Para. 12.8; MAS Notice 1014 Para. 12.8; MAS Notice 824 Para. 11.4; MAS Notice SFA04-N02 Para. 10.8; MAS Notice FAA-N06 Para. 10.8, MAS Notice 314 Para. 10.8; MAS Notice 3001 Para. 10.8; MAS Notice TCA-N03 10.8; MAS Notice SFA13-N01 Para 7.4.

the AML/CFT compliance officer are contained in the MAS Guidelines. This guidance relates to the following issues:

(a) Ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected.

(b) Advising and training senior management and staff on the development and implementation of internal AML/CFT policies, procedures and controls.

(c) Carrying out, or overseeing the carrying out of, ongoing monitoring of business relations and sample reviewing of accounts for compliance with the MAS Notices and Guidelines.

(d) Promoting compliance with the MAS Notices and Guidelines, including in particular observance of the underlying principles on AML/CFT in the MAS Notices and taking overall charge of all AML/CFT matters within the organisation.[68]

526. Financial institutions are required to ensure that the AML/CFT compliance officer and any other persons appointed to assist him/her have timely access to all customer records and other relevant information which would be required for them to discharge their duties.[69]

527. MAS Notices require financial institutions to maintain an audit function that is adequately resourced and independent. The audit function should regularly assess the effectiveness of the financial institution's internal policies, procedures and controls, and its compliance with regulatory requirements.[70]

528. MAS Notices require financial institutions to take all appropriate steps to ensure that their staff and agents, whether located in Singapore or overseas, are regularly trained on:

(a) AML/CFT laws and regulations, in particular, CDD measures, detecting and reporting of suspicious transactions.

(b) Prevailing ML/FT techniques, methods and trends.

(c) The financial institutions' internal AML/CFT policies, procedures and controls, including the related roles and responsibilities of staff and agents.[71]

529. To help ensure the effectiveness of training, financial institutions are required to monitor training attendance and take appropriate follow-up action in respect of those who missed such training without reasonable cause. Apart from the initial training, financial institutions are required to provide refresher training at regular intervals to ensure that staff are reminded of their responsibilities and are kept informed of developments. Refresher training should be held at least once every two years.[72]

---

[68] MAS Guidelines 626 Para. 66; MAS Guidelines 1014 Para. 66; MAS Guidelines 824 Para 66; MAS Guidelines SFA04-N02 Para. 66; MAS Guidelines FAA-N06 Para. 62; MAS Guidelines 314 Para. 60; MAS Guidelines 3001 Para. 49; MAS Guidelines TCA-N03 Para. 54; MAS Guidelines SFA13-N01 Para. 29.

[69] MAS Notice 626 Para. 12.9; MAS Notice 1014 Para. 12.9; MAS Notice 824 Para. 11.5; MAS Notice SFA04-N02 Para. 10.9; MAS Notice FAA-N06 Para. 10.9; MAS Notice 314 Para. 10.9; MAS Notice 3001 Para. 10.9; MAS Notice TCA-N03 Para. 10.9; MAS Notice SFA13-N01 Para. 7.5.

[70] MAS Notice 626 Para. 12.10; MAS Notice 1014 Para. 12.10; MAS Notice 824 Para. 11.6; MAS Notice SFA04-N02 Para. 10.10; MAS Notice FAA-N06 Para. 10.10; MAS Notice 314 Para. 10.10; MAS Notice 3001 Para. 10.11; MAS Notice TCA-N03 Para. 10.10; MAS Notice SFA13-N01 Para. 7.6).

[71] MAS Notice 626 Para. 12.12; MAS Notice 1014 Para. 12.12; MAS Notice 824 Para. 11.8; MAS Notice SFA04-N02 Para. 10.12; MAS Notice FAA-N06 Para. 10.12; MAS Notice 314 Para. 10.12; MAS Notice 3001 Para. 10.13; MAS Notice TCA-N03 Para. 10.12; MAS Notice SFA13-N01 Para. 7.8.

[72] MAS Guidelines 626 Para. 67 – 68; MAS Guidelines 1014 Para. 67 – 68; MAS Guidelines 824 Para. 67 – 68; MAS Guidelines SFA04-N02 Para. 67 – 68; MAS Guidelines FAA-N06 Para. 63 – 64; MAS Guidelines

530. Financial institutions are also required to have in place screening procedures to ensure high standards when hiring employees and agents, which include checking with former employers, referees and pre-employment screening agencies.[73]

Effectiveness

531. Recently, moneylenders became subject to requirements to implement internal control programmes that substantially meet the FATF Recommendations. However, at this early stage, it is not yet possible to assess the effectiveness of their implementation.

532. Recommendation 15 is being implemented effectively in the other financial sectors. MAS has been determining, through on-site examinations, the adequacy of the financial institution's policies and procedures with regard to areas such as CDD, record keeping, monitoring of accounts, reporting of suspicious transactions, and training. Examiners review the financial institution's audit, examination and other relevant reports to obtain an overview of the institution's control environment and effectiveness of the measures taken to counter ML/FT. Based on the review, they have been assessing whether there were recurring weaknesses and whether remedial procedures have been adequate to control the risk. They have also been reviewing management's response to audit findings for an indication of management's control consciousness and willingness to implement controls, as well as the activities, roles and responsibilities of the compliance officer or unit responsible for monitoring ML/FT activities in the financial institution.

533. Financial institutions explained to the onsite assessment team that they have put in place a process for conducting testing, and measuring the effectiveness of internal controls. Their management supervises the day-to-day activities of employees to ensure that adequate infrastructure and internal controls are in place. They have been auditing AML/CFT requirements on a group-wide basis with established frequencies according to the risk assessment of each auditable activity or unit. Compulsory AML training programs have been provided to new staff and agents and those employees involved in dealing with customers or processing customers' transactions, and tracking mechanisms are in place to determine staff and agents that have either not attended or completed the training. Non-attendees or those who fail are escalated to senior management for remediation. They have also indicated that they have established pre-employment screening procedures to reference-check adverse status or backgrounds of staff and agents being recruited with previous employers or other sources for credit delinquency, bankruptcy, litigation or other relevant records.

Recommendation 22

534. Financial institutions incorporated in Singapore are required to develop their group policies on AML/CFT and extend them to all of their branches and subsidiaries which are located outside of Singapore. They are also required to ensure that their foreign branches and subsidiaries adhere to head office/group policy. Group policies do not apply to finance companies and approved trustees as they only have a local presence.[74]

535. Where financial institutions have branches or subsidiaries in a host country or jurisdiction that is known to have inadequate AML/CFT measures (as determined by the financial institutions for themselves or notified to financial institutions generally by MAS or by other foreign regulatory

---

314 Para. 61 – 62; MAS Guidelines 3001 Para. 50 – 51; MAS Guidelines TCA-N03 Para. 55 – 56; MAS Guidelines SFA13-N01 Para. 30 – 31.

[73] MAS Notice 626 Para. 12.11; MAS Notice 1014 Para. 12.11; MAS Notice 824 Para. 11.7; MAS Notice SFA04-N02 Para. 10.11; MAS Notice FAA-N06 Para. 10.11; MAS Notice 314 Para. 10.11; MAS Notice 3001 Para. 10.12; MAS Notice TCA-N03 Para. 10.11; MAS Notice SFA13-N01 Para. 7.7.

[74] MAS Notice 626 Para. 12.4; MAS Notice 1014 Para. 12.4; MAS Notice SFA04-N02 Para. 10.4; MAS Notice FAA-N06 Para. 10.4; MAS Notice 314 Para. 10.4; MAS Notice 3001 Para. 10.4; MAS Notice TCA-N03 Para. 10.4).

authorities), they are required to ensure that their group policies on AML/CFT are strictly observed by the management of the branches or subsidiaries.[75] Where the AML/CFT requirements in the host countries or jurisdictions differ from those in Singapore, financial institutions shall require that the overseas branches or subsidiaries apply the higher of the two standards, to the extent that this is permitted by the law of the host countries or jurisdictions.[76]. Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the head office of the financial institution is required to report to MAS and comply with any further directions given by it.[77]

Effectiveness

536. Recently, moneylenders became subject to requirements to implement group policies for their foreign branches and subsidiaries, which substantially meet the FATF Recommendations. However, at this early stage, it is not yet possible to assess the effectiveness of their implementation. Recommendation 22 is being effectively implemented in the other financial sectors. In the course of its inspections, MAS ascertains whether the group AML/CFT policy has been communicated to the management of the financial institution's overseas offices. MAS also reviews the minutes of meetings of AML/CFT committees or task forces that may have been established at the head office level, or of any meetings during which ML/FT issues were discussed, including those relating to foreign branches and subsidiaries. MAS examiners determine how the board of directors and senior management ensure that the overarching AML/CFT policies of Head Office are implemented effectively across the businesses and in all jurisdictions. MAS indicated that it has received no notification under paragraph 12.7 of the MAS 626, that the law of a host country conflicts with Singapore law, such that the overseas branch or subsidiary cannot observe the higher standard.

537. Financial institutions with which the assessment team met confirmed that they have been establishing and implementing global AML policies and measures that have been applied consistently among their foreign branches or subsidiaries, in which they check for compliance against both home and host country AML standards and adopt the higher of the two standards.

3.8.2 Recommendations and Comments

538. Moneylenders were very recently made subject to requirements to implement internal control programs (Recommendation 15). The authorities should ensure that they effectively implement these obligations going forward. Commodities futures brokers should be made subject to the requirements under Recommendation 22.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**LC**	• Commodities futures brokers will only be covered in 2008. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
R.22	**LC**	• Commodities futures brokers will only be covered in 2008 effectiveness.

[75] MAS Notice 626 Para. 12.5; MAS Notice 1014 Para. 12.5; MAS Notice SFA04-N02 Para. 10.5; MAS Notice FAA-N06 Para. 10.5; MAS Notice 314 Para. 10.5; MAS Notice 3001 Para. 10.5; MAS Notice TCA-N03 Para. 10.5.

[76] MAS Notice 626 Para. 12.6; MAS Notice 1014 Para. 12.6; MAS Notice SFA04-N02 Para. 10.6; MAS Notice FAA-N06 Para. 10.6; MAS Notice 314 Para. 10.6; MAS Notice 3001 Para. 10.6; MAS Notice TCA-N03 Para. 10.6.

[77] MAS Notice 626 Para. 12.7; MAS Notice 1014 Para. 12.7; MAS Notice SFA04-N02 Para. 10.7; MAS Notice FAA-N06 Para. 10.7; MAS Notice 314 Para. 10.7; MAS Notice 3001 Para. 10.7; MAS Notice TCA-N03 Para. 10.7.

3.9 Shell Banks (R.18)

3.9.1 Description and Analysis

Recommendation 18

539. There are no shell banks that are legally authorised to operate in Singapore. It has been MAS's long-established policy not to allow their establishment. MAS Notices define a "shell bank" as a bank incorporated, formed or established in a country or jurisdiction where the bank has no physical presence and which is unaffiliated to a regulated financial group (MAS Notice 626 Para. 8.2(e); MAS Notice 1014 Para. 8.2(e).

540. MAS affirms that, even though there are no specific provisions in the Banking Act, Regulations or Notices that prohibit the establishment of shell banks in Singapore, the policy has been effectively implemented through stringent requirements under the MAS Bank Admission Framework to disqualify a shell bank from obtaining a banking license in Singapore. These requirements include Head Office reputation and track record, business plan, financial resources, shareholder, ownership structure and reputation of major shareholders/controllers, management and staff expertise, corporate governance, funding systems and control, home country supervision and systemic impact.

541. In addition, the Bank Admission Framework requires the applicant to submit audited financial statements for the last three years as well as a confirmation from its home supervisor that the proposed Singapore entity will be subject to its consolidated supervision. The MAS approval is valid for one year in the first instance and the applicant must establish a physical presence in Singapore with substantive operations. It also needs to seek MAS' approval for appointment of senior executives who are required to be based in Singapore, and inform MAS of the date of commencement of business.

542. Banks in Singapore are prohibited from entering into or continuing correspondent banking relations with a shell bank (MAS Notice 626 Para. 8.6; MAS Notice 1014 Para. 8.6).

543. Banks are required to take appropriate measures when establishing correspondent banking relations to satisfy themselves that their respondent banks do not permit their accounts to be used by shell banks (MAS Notice 626 Para. 8.7; MAS Notice 1014 Para. 8.7).

Effectiveness

544. During on-site inspections, MAS examiners have been ascertaining that banks are aware of the possible risks relating to opening correspondent banking accounts and that their policies and procedures highlight these risks. For example, examiners assess if banks have checked whether the respondent banks dealt with shell banks and if so, whether they have terminated the correspondent banking relationship. Examiners also verify if banks have exercised due diligence and assessed the level of perceived risk associated with each respondent bank and adopted enhanced due diligence for higher risk respondent banks. No cases of shell banks have arisen from on-site inspections.

545. Banks interviewed during the onsite visit indicated that in the process of assessing suitability of the respondent bank and documenting the respective AML/CFT responsibilities of each bank, they have been ascertaining if the respondent bank has maintained any physical presence, and whether it has established any relations with a shell bank. They stated clearly that they have been perceiving international correspondent banking as one of the business areas particularly susceptible to money laundering or terrorist financing.

3.9.2 Recommendations and Comments

546. Singapore's use of the licensing system for financial institutions to uncover shell bank operations seems to be working effectively. However, for the sake of clarity, it is recommended that Singapore consider expressly prohibiting the operation of shell banks.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**C**	• This Recommendation is fully observed.

Regulation, supervision, guidance, monitoring and sanctions

3.10 The Supervisory and Oversight System - Competent Authorities and SROs: Role, Functions, Duties and Powers (Including Sanctions) (R.23, 30, 29, 17, 32 & 25)

3.10.1 Description and Analysis

Authorities/SROs roles and duties & Structure and resources - R.23, 30

Recommendation 23 (Supervisory authorities)

Designated supervisory authorities and application of AML/CFT measures

547. A full range of financial institutions, including those in the banking, insurance, securities and futures, money changing and remittance businesses and trust companies are subject to AML/CFT measures, including CDD, record keeping and STR reporting requirements. At present, only commodity futures brokers are not yet subject to specific AML/CFT obligations other than the STR reporting requirements. Commodity futures brokers will have their licences transferred to a MAS Capital Markets Services licence under the Securities and Futures Act as of February 2008 and will have to comply with the MAS AML/CFT Notice SFA04-N02 for CMS licensees. Moneylenders are regulated under the Moneylenders Act which is under the purview of the Ministry of Law. Under the new rule-making power introduced to the Act in 2006, the Ministry of Law together with the Registrar of Moneylenders issued AML/CFT rules for moneylenders which entered into force on 12 November 2007.

548. The Monetary Authority of Singapore (MAS) is both the central bank and integrated regulator that exercises supervisory oversight responsibilities over the banking, insurance, securities and futures industries through the MAS Act, Banking Act, Finance Companies Act, Insurance Act, Securities and Futures Act and Financial Advisers Act. Additionally, it is responsible for licensing money-changers and remittance agents (pursuant to the Money-Changing and Remittance Businesses Act) and trust companies (pursuant to the Trust Companies Act). From early 2008, MAS will also have regulatory oversight of commodity futures trading in Singapore. MAS is also responsible for ensuring that Singapore-incorporated financial institutions are requiring that their branches or subsidiaries overseas observe their group AML/CFT policy. Moneylenders are under the purview of MINLAW. For a full discussion, see section 3.8 of this report.

Structure and resources of supervisory authorities

Supervisors – Structure, funding and resources

549. MAS enjoys operational autonomy. Under the MAS Act, the Board of Directors of MAS is appointed by the President. The Chairman of the Board is appointed by the President, on the recommendation of the Cabinet. The Board of Directors is responsible for the policy and general administration of the affairs and business of MAS and informs the Government of the banking and credit policy of MAS. The director appointed is not permitted to serve on the board of any commercial, financial, agricultural, industrial or other interests that could be connected to MAS (Para 8 (2b), MAS Act). The Board is ultimately accountable to the Parliament of Singapore through the Minister in charge of MAS who is Singapore's current Senior Minister.

550. MAS sets its own budget and hires the staff it requires to perform its supervisory functions. Being a self-funded statutory board, MAS' budget is approved by the MAS Board (and only subject to the President's approval if the budget encroaches on past Government reserves). MAS' core activities

include supervision of banks, insurance and the securities and futures industries, the conduct of monetary policy and issuance of currency, management of the official foreign reserves, fiscal agent to the Government and the promotion of a sound and progressive financial centre. MAS' annual household budget for the past 3 years is shown in the table below. On average, the costs of supervision of the banking, insurance and securities and futures industries and market conduct of licensed financial advisors and insurance intermediaries take up almost 50% of household expenses, which is about SGD 110 million per annum.

			$'000
Household Budget	FY05/06	FY06/07	FY07/08
Personnel Expenditure	141,669	134,985	151,936
General and Administrative Expenditure	43,136	50,068	51,600
Depreciation/amortisation	26,000	28,000	28,000
MAS Household Budget	**210,805**	**213,053**	**231,536**

551. Of the 705 professional staff of MAS, roughly 50% (364 persons) have been assigned to the two departments of Prudential Supervision and Market Conduct that make up the Financial Supervision Group (comprising Banking Supervision, Complex Institutions Supervision, Capital Markets, Capital Markets Intermediaries, Insurance Supervision, Prudential Policy and Specialist Risk Supervision). Roughly 200 of the 364 persons are supervisors. The following chart sets out the number of staff who are responsible for conducting on- and off-site inspections of each type of financial institution.

Type of institution	Number of licensees for each type of institution	Number of MAS staff responsible for supervising those institutions	Number of supervisors with specialist AML/CFT knowledge	% of supervisors with specialist AML/CFT Knowledge
Banks / Merchant Banks	161	117	30	26%
Finance Companies	3			
Money-changers & remittances agents	470			
Capital Markets Services Licensees	197	70	16	23%
Financial Advisers & Insurance Intermediaries	133			
Trust companies	36			
Life insurers*	17	12	4	33%

Figures are of 14 November 2007.

* Life insurers that are subsidiaries of the local banks are regulated by staff regulating local banks, under banks/merchant banks category.

552. In their work of AML/CFT supervision of financial institutions, the supervisors have a full range of guidance at hand:

- Examination Manual – AML/CFT
  - Provides an overview of the AML/CFT regime in Singapore.
  - Highlights high risk products and services that are more vulnerable to money laundering, as well as the inherent risks and risk management controls in AML/CFT.

- Sets out the basic principles to apply in combating money laundering, including KYC, enhanced due diligence for higher risk customers such as PEPs and correspondent banking, suspicious transactions monitoring, AML/CFT training and record retention.
- Outlines detailed examination procedures which supervisors use for on-site visits.

- Self Assessment Questionnaire on AML/CFT
  - Facilitates offsite review of the AML/CFT measures implemented by financial institutions.
  - Input for preparing an inspection or a supervisory visit.

- Financial Supervision Group Faculty of Peers – AML/CFT
  - Group of MAS experts on AML/CFT.
  - Resources available: examination manuals, FATF regulations & assessment methodology, BIS and FATF papers.
  - Provides support and guidance to MAS supervisors on AML/CFT issues.

553. Overall, MAS is adequately staffed, and has sufficient technical and other resources, including expertise on AML/CFT policies and measures, to fully perform its AML/CFT functions.

Supervisory staff – Professional standards, skills and confidentiality

554. MAS has staff with specialist knowledge in AML/CFT policies and measures across the organisation, particularly in the departments which conduct on- and off-site inspections of financial institutions (see preceding section). MAS staff are required to comply with MAS' internal policies and procedures which set out standards to ensure professionalism and a high level of integrity. On appointment, all employees are required to complete an undertaking to safeguard official documents and information, acquired in his/her official capacity, during and after their service as MAS employees (under the Official Secrets Act). Once every three years, employees are required to renew this undertaking. The undertaking includes the agreement to comply with statutory requirements under the Official Secrets Act, the Statutory Bodies and Government Companies (Protection of Secrecy) Act, the MAS Act and the Computer Misuse Act (Statutory Requirements for Secrecy of Information and Instructions for the Handling and Custody of Classified Documents and Information) as set out in Operations and Procedures, Para. 2.5 in MAS OPM 3/II/A.

555. In addition, the MAS Code of Conduct was launched in May 2007. The Code is driven by MAS' core value of integrity that is a pre-requisite for the high standards of ethical and professional conduct expected in the Code. The Code also serves as a guide in addressing ethical issues or conflicts of interest situations and sets out the guiding principles deriving from the value of integrity. Existing employees as well as new staff as of May 2007 are required to declare their commitment to the Code. Staff also undergo a one month induction programme, screening by ISD on staff who needs to have access to secret information, and a stringent recruitment process to ensure that they are of the highest integrity.

556. AML/CFT training is part of the formal training roadmap for all MAS supervisory staff. Such training is structured. For new entrants, on-the-job training and working under an experienced team leader provide the officers with guidance and direction in investigative techniques. MAS' banking and complex institutions supervisory department officers also attend the Regional Banking Supervisory Programme, which has a module on AML, as well as other AML/CFT-related conferences and seminars in Singapore and abroad.

557. Within the organisation, MAS holds training sessions that are specifically focused on AML/CFT, for both new staff and those who do not have specialist knowledge in this area. External speakers (*e.g.* from CAD) and MAS staff with specialist knowledge in AML/CFT policies and measures as well as external speakers have led such training sessions. To upgrade and sharpen the supervisory skills of its staff, MAS spent SGD 2.8 million in 2006 to provide regular training, including AML/CFT training. MAS officers regularly attend international and domestic conferences as

well as training workshops relating to AML/CFT. Upon their return from such courses, participants conduct presentations to share their learning with other colleagues.

558. An AML/CFT Faculty of Peers Group (within the Financial Supervision Group) has been set up as part of the piloted Faculty of Peers Project. This AML/CFT Faculty of Peers Group consists of: (1) Faculty Practice Area Leaders, who are actively involving in workgroups or leading inspection teams relating to AML/CFT; and (2) experienced Peers who are actively involved in AML/CFT work through their portfolio or projects. The initiatives taken by this Group to date include reviewing the AML/CFT Notices and Guidelines, contributing materials to the hotline database and informing MAS officers of updates on the AML/CFT examination manuals, FATF Recommendations and Basel Committee of Banking Supervision papers. The MAS also has a range of supervisory tools and guidance materials to supplement and assist the examiners on their supervisory work on AML/CFT, such as: databases on AML/CFT Regulations and Guidance, and AML/CFT Inspection Findings; an AML/CFT Examination Manual; an AML/CFT questionnaire to be completed by financial institutions; and operational procedure manuals on procedures relating to STRs. Additionally, MAS officers can access on-line AML/CFT training programmes available on FSI Connect.

Authorities Powers and Sanctions – R.29 & 17

Recommendation 29 (Supervisory powers)

General monitoring powers and on-site inspection authority

559. MAS has a broad range of powers to monitor and ensure financial institutions' compliance with AML/CFT measures, including powers of off-site surveillance, auditing and on-site visits and inspections. MAS conducts off-site surveillance by requesting financial institutions to complete an AML/CFT questionnaire that seeks to obtain information on the financial institutions' exposure to the ML/FT risks. This questionnaire was sent to almost all banks, life insurers and capital markets services licensees in 2007. Intermediaries that engage in activities that pose a higher AML/CFT risk are required to submit this questionnaire once every two years. In the banking sector, it is sent and received, on average, once every two years. MAS intends to review, on a risk-based approach, how frequently to update the questionnaire for capital markets intermediaries and life insurers. The AML/CFT questionnaire serves as a tool for the financial institution to assess the adequacy and effectiveness of its AML/CFT measures and controls. MAS reviews the completed questionnaire and, where necessary, follows up with further inquiry (*e.g.* obtaining a copy of the financial institution's procedural manual). MAS may select financial institutions for inspection based on such reviews. Also, MAS periodically meets the financial institutions' senior management staff, compliance and audit heads to get a sense of the effectiveness of the AML/CFT framework through discussions with them.

560. MAS also uses financial institutions' internal and external auditors to review their institution's compliance with AML/CFT requirements. If an external auditor, in the course of performing his duties as an auditor of a bank, is satisfied that there has been a serious breach or non-observance of the provisions of the Banking Act or that a criminal offence involving fraud or dishonesty has been committed, he shall immediately report the matter to the MAS. Similar provisions apply to other financial institutions.[78] MAS may (or may require the financial institution to) appoint an independent person to submit an audit report and confirm that the financial institution is not contravening any relevant laws and regulations: section 44A(3), Banking Act; section 41(5), Finance Companies Act; section 36(9), Insurance Act; sections 109 and 115, Securities and Futures Act; section 26(2), MCRBA; section 50, Financial Advisers Act; section 32, Trust Companies Act.

[78] S.58(8), Banking Act; s.41(7), Finance Companies Act; s.108, Securities and Futures Act; s.49, Financial Advisers Act; s.36(11), Insurance Act; s.26(2), MCRBA; Regulation 6, MCRBA Regulations 2005; s.31, Trust Companies Act.

561. Section 27B MAS Act vests MAS with a broad power to issue such directions or make such regulations concerning any financial institution or class of financial institutions as MAS considers necessary for the prevention of money laundering or for the prevention of the financing of terrorism. This power seems broad enough to cover the provisions in the MAS AML/CFT Notices obliging financial institutions to extend their group policies on AML/CFT to all of their branches and subsidiaries outside Singapore.

562. MAS has the power to conduct on-site inspections and supervisory visits to financial institutions to examine their AML/CFT controls and procedures. The scope of MAS inspection includes the review of the financial institutions' policies and procedures, books and records, and sample or transaction testing.[79]

563. MAS' inspection powers with respect to trust companies as well as to money changing and remittance businesses seem confined to compliance with the respective Acts, and thus without inclusion of monitoring the compliance with MAS Notices on AML/CFT. MAS has put forward the argument that part and parcel of its supervisory mandate includes monitoring that institutions have robust AML/CFT systems and procedures in place. It considers that this covers its authority to inspect for compliance with AML/CFT regulations and to impose sanctions in case of non-compliance, even in the absence of an explicit power in the relevant Acts or in the AML/CFT Notices issued to such sectors on the basis of section 27B of the MAS Act.

564. A monograph entitled "Objectives and Principles of Financial Supervision in Singapore", issued by MAS in April 2004 and published on its website, states: *"At the same time as it supervises the safety and soundness of financial institutions, MAS also requires institutions to have in place robust systems and procedures to combat money laundering and terrorism financing."* At the second reading in Parliament of the Trust Companies Bill and the Money-Changing and Remittance Businesses (Amendment) Bill, respectively, in 2005, the introducing minister of both bills brought home that one of the reasons, if not the main one, for the legislative changes was the strengthening of the AML/CFT system in the respective fields. In the second reading of the MCRB (Amendment) Bill, the minister said: "*That amendments aim to refine and better reflect MAS' supervisory approach towards holders of remittance licences and money-changing licences. I should state at the outset that MAS' supervision of these activities focuses on anti-money laundering and countering the financing of terrorism. MAS does not supervise holders of these licences for their safety and soundness. This approach of focusing on anti-money laundering rather than safety and soundness of remittance houses and money changing operations is similar to those adopted by other reputable financial centres."*

565. Accordingly, MAS is of the opinion that its supervisory mandate encompasses the policing the systems of these sectors for AML/CFT and that MAS' inspections of these sectors for compliance with the relevant AML/CFT Notices is consistent with the object of regulating and supervising these sectors. However, for the avoidance of doubt, MAS has, on 8 October 2007, imposed additional licensing conditions on trust companies and money changing and remittance sector to provide greater clarity on MAS' power to inspect them for AML/CFT breaches and to remind them of their obligations and responsibility of ensuring compliance with these requirements. Such additional conditions enable MAS explicitly to inspect these sectors or require them to furnish information for the purpose of MAS' monitoring their level of compliance with the relevant MAS AML/CFT Notices. Interviews with relevant private sector entities have confirmed that MAS is actually monitoring the entities' compliance with the relevant MAS AML/CFT Notices.

[79] S.43, Banking Act; s.33, Finance Companies Act; s.150 and 290, Securities and Futures Act; s.70, Financial Advisers Act; s.40, Insurance Act; s.18, MCRBA; s.40, Trust Companies Act.

Power to compel production of or obtain access to information

566. MAS has the power to require a financial institution to produce its books, accounts and documents, and to afford MAS access to such information or facilities as may be required to conduct the inspection or investigation. As MAS' powers to compel production of or to obtain access to all records, documents or information relevant to monitoring compliance under the TCA and the MCRBA seem to be confined to compliance with these Acts, there are concerns about MAS' power to compel production of or obtain access to all records, documents or information relevant to monitoring compliance with the MAS AML/CFT Notices for the relevant sectors under section 18 of the MCRBA and section 40 of the TCA and to impose sanctions in case of non-compliance. Arguing that MAS' inspections of these sectors for compliance with the relevant AML/CFT Notices is consistent with the object of regulating and supervising these sectors, AGC argued that MAS may compel production of, or obtain access to, records, documents or information for monitoring compliance with the relevant MAS AML/CFT Notices on the basis of more general provisions of the relevant Acts, namely section 17 MCRBA which requires a licensee to furnish to MAS such returns and information as the Authority may reasonably require "for the proper discharge of its functions" and section 28(5) TCA which requires a licensee to furnish to MAS such returns and information as the Authority may require. Additional licensing conditions were imposed on all licensees on 8 October 2007 which explicitly provide for MAS' inspection of these sectors and the requirement to furnish information for the purpose of assisting MAS in monitoring the licensees' level of compliance with the relevant MAS AML/CFT Notices.

567. Any financial institution that, without reasonable excuse, does not produce the information as required by MAS to conduct the inspection or investigation will be guilty of an offence and shall be liable on conviction to a fine (of which the maximum is stated in the relevant legislation.[80]

568. MAS Notices also require financial institutions to submit reports on suspicious transactions (including attempted transactions) to STRO and extend a copy to MAS for information.[81]

569. MAS' power to compel production of or to obtain access for the purpose of inspection or investigation of the relevant financial institutions is not predicated on the need to require a court order.[82]

Powers of enforcement and sanction

570. There is a range of criminal, regulatory and supervisory measures available against financial institutions for failure to comply with or properly implement their AML/CFT obligations. Additionally, a director, managing director, and a varying range of management personnel and in some cases officers of the financial institution may be personally liable if they fail to take all reasonable steps to secure compliance by a financial institution with the relevant Acts. However, as only the Banking Act, the Securities and Futures Act and the Finance Companies Act extend this liability beyond the respective Acts to other laws relating to such companies, it seemed – at the time of the onsite visit – that personal liability of directors and senior management personnel for failure to comply with or properly implement the MAS AML/CFT Notices was not generally foreseen, as some Acts did not extend the liability beyond the respective Acts, and the wording of the ones that did gave rise to the question of whether the MAS AML/CFT Notices could be qualified as other laws. Under the

---

80 Sections 43-44A, Banking Act; s.33, Finance Companies Act; s.150, 152, 163 and 290, Securities and Futures Act; s.70–72, Financial Advisers Act; s.40–40A, Insurance Act; s.17, MCRBA; s.28(5) and (8), Trust Companies Act.

81 MAS 626 Para. 11.2; MAS 824 Para 10.2; MAS SFA13-N01 Para. 6.2; MAS 1014 Para 11.2, MAS 3001 Para. 9.2; MAS SFA04-N02 Para 9.2; MAS FAA N06 Para. 9.2; MAS TCA TCA-N03 Para 9.2; MAS 314 Para. 9.2.

82 S.43 - 44A, Banking Act; s.33, Finance Companies Act; s.150, 152, 163 and 290, Securities and Futures Act; s.70 – 72, Financial Advisers Act; s.40 – 40A, Insurance Act; s.17, MCRBA; s.28(5) and (8), Trust Companies Act.

various legislations, the directors and management personnel may be liable on conviction to a fine of varying maximum amounts, but not exceeding SGD 125 000 and/or imprisonment for varying terms, but not exceeding three years.[83]

571. MAS may also direct the removal of a chief executive or officer, or issue him/her a formal reprimand, if MAS is satisfied that they wilfully contravened or caused the financial institution to contravene the AML/CFT regulations.[84] For Money-changers and Remittance Businesses, whose licenses have to be renewed annually, MAS has the power not to renew them if it is not satisfied as to, inter alia, the character of the management of the company.

Recommendation 17 (Sanctions)

572. Singapore has implemented criminal and administrative sanctions to deal with natural or legal persons who are covered by the FATF Recommendations and fail to comply with national AML/CFT requirements. MAS is the authority responsible for applying all non-criminal sanctions. Generally, criminal sanctions are sought by the Public Prosecutor and imposed by the courts after conviction.

Criminal sanctions

573. It is a criminal offence to fail to disclose knowledge or suspicion that property is the proceeds of crime (s.39(2) CDSA). The CAD has charged a person under this provision for failing to report a STR. This case was pending trial at the time of the on-site visit. The TSOFA also contains a number of offences for failing to disclose information related to terrorist financing.

574. In addition, Section 27B(2), MAS Act stipulates that a financial institution which fails or refuses to comply with any direction issued under section 27B(1), MAS Act shall be liable to a fine of up to SGD 1 million and in case of a continuing offence, to a further fine of SGD 100 000 for everyday during which the offence continues after conviction. Directors and officers may be criminally liable where non-compliance of the financial institution with the Act is attributable to their consent, connivance or neglect (s.28B MAS Act). As of November 2007, no criminal sanctions had yet been applied to any financial institutions. However, action had been taken through a range of supervisory measures mechanisms (*e.g.* administrative sanctions such as warning letters).

Administrative sanctions

575. MAS has the authority to apply a broad range of measures ranging from administrative sanctions to revocation of license for AML/CFT contraventions. The MAS Act (s.27(1)) indicates that the authority may request information and make recommendations to such financial institutions as MAS may, from time to time, determine and may issue directions for the purpose of securing that effect is given to any such request or recommendation. Criminal penalties (a fine of up to SGD 20 000) apply for failure to comply. Section 27B further provides the power to issue directions to financial institutions to combat ML/FT, with criminal penalties (a fine of up to SGD 1 000 000, and an additional daily fine of SGD 100 000 for each additional day of non-compliance) for failure to comply. These two powers combined could give the authority to MAS to notify the financial institution or make any recommendation that it sees fit. This broad power thus includes the ability to issue a warning or reprimand letter, which could indicate specific deficiencies that need to be rectified, order a change in management, suspend or withdraw a license, or issue a fine. A failure to comply with those actions/notifications could then eventually result in the criminal sanction under 27(1) or 27B. The

[83] S.66, Banking Act; s.49, Finance Companies Act; s.332, Securities and Futures Act; s.84, Financial Advisers Act, s.55(3), Insurance Act; s.21, MCRBA; s.65, Trust Companies Act.

[84] Regulation 18A, Banking (Corporate Governance) Regulations for banks incorporated in Singapore; Paragraph 7 MAS Notice 622A on Appointment of Chief Executives of Branches of Banks Incorporated Outside of Singapore; s.31(4) Insurance Act; s.44(1), 81A, 81ZJ and 97 Securities & Futures Act; s.57(1) Financial Advisers Act; s.14(1) Trust Companies Act; s.7 and 7(A) Money-changing and Remittance Businesses Act.

MAS advises that such reprimands have, in fact, been issued to, and accepted by, various financial institutions in the past. As indicated below, these administrative sanctions have been applied to specific breaches of the AML/CFT Notices.

576. MAS applies its range of administrative sanctions with the objective of getting financial institutions to remedy the deficiencies in their internal control systems. This is a key component of MAS' post-inspection process.

577. In the course of on-site inspections, MAS examiners comment on the financial institutions' compliance with AML/CFT regulations as well as their risk management systems and controls, and require the financial institutions' management to rectify the deficiencies noted, normally within a time frame of 3 to 6 months. For major system changes or the procurement of additional resources, the financial institution might be given more time, but will have to put in place interim compensating controls to mitigate the ML/TF risks. MAS may also address significant examination findings and remedial actions to the chairman of the financial institution and specifically require the board of directors to ensure that the financial institution rectifies the weaknesses highlighted. The financial institutions' responses to the inspection findings are submitted to MAS in writing. In the case of financial institutions under the consolidated supervision of foreign regulatory authorities, MAS also sends inspection reports to their head offices and parent regulators. In addition, MAS follows up on the examination findings to ensure that the deficiencies have been rectified. MAS may also request the financial institution's external auditors to follow up on the MAS' inspection findings and the adequacy of any rectifications.

578. MAS also follows up on the breaches noted. In determining the regulatory action to be taken, MAS would take into consideration the severity of the breach and the circumstances related to the breach.

579. MAS reports that administrative sanctions such as a letter of reprimand or letter requiring remedial action have been very effective in getting financial institutions to rectify their breaches and deficiencies. Financial institutions under the consolidated supervision of foreign regulatory authorities operating in Singapore are required to send a copy of the reprimand letter or letter requiring remedial action to their Head Offices, together with the explanation on the breaches and rectifications.

580. MAS has authority in other laws to impose sanctions on financial institutions as well. MAS may at any time vary or revoke any existing conditions of a licence or impose conditions or additional conditions such as ring-fencing measures to restrict the operation of the financial institutions. [85] For example, MAS has in the past imposed ring-fence measures such as restrictions on deposit taking for prudential reasons. Additionally, MAS has the power to revoke the license of financial institutions or representatives of financial institutions if they fail to comply with their AML/CFT obligations or are acting in a manner detrimental to depositors' interest.[86]

Sanctions applying to directors and senior management

581. The MAS Act was amended through the MAS (Amendment No. 2) Act 2007 with a new section 28B on corporate offenders and unincorporated associations which creates a derivative liability in the MAS Act on officers (directors, members of the committee of management, chief executive, manager, secretary or other similar officers) where non-compliance by a financial institution is attributable to their consent, connivance or neglect. Read in conjunction with section 27B of the MAS Act, this amendment creates a derivative liability for officers in the afore-mentioned circumstances where a financial institution fails or refuses to comply with the MAS AML/CFT directions or

[85] S.7(4), Banking Act; s.30, 7 and 7(A), MCRBA; s.6(4), Finance Companies Act; s.88(2), Securities and Futures Act; s.10(1), Insurance Act; s.7, Trust Companies Act.

[86] S.20, Banking Act; s.15, Finance Companies Act; s.95(2) and 289(4), Securities and Futures Act; s.19 (2), Financial Adviser Act; s.12 and 12A, Insurance Act; s.14(5), MCRBA; s.10(2) Trust Companies Act.

regulations. The officer would be liable to the same sanctions as are applicable to the financial institution, i.e. a fine not exceeding SGD 1 million and, in the case of a continuing offence, to a further fine of SGD 100 000 for every day during which the offence continues after conviction. The amendment was gazetted on 19 October and entered into force on 1 November.

Overview of actions taken against financial institutions for non-compliance with AML/CFT Notices from 2004 to 14 November 2007*

	Banks, Merchant Banks, Finance Companies, Capital Markets Intermediaries and Financial Advisers	Money Changers / Remittance Businesses
Serious warning / reprimand letter	5	-
Change in senior management/ Summoned senior management for reprimand or caution/ Required presence of regional management in Singapore	14	-
Informed parent supervisor to convey specific concerns	9	-
Required independent review of AML/CFT procedures and controls by internal/external auditors	7	-
Curbed business expansion plans until AML/CFT controls were strengthened	17	-
Required to increase compliance resources	12	-
Fines	-	92
Revocation of License	-	2
Non-renewal of License	-	8
Referred matter to CAD	2	3

*Figures relate to the number of breaches, not the number of entities against which action was taken.

582. In considering the appropriate sanction to be meted out, MAS takes into consideration the severity of the breaches or deficiencies, the root cause of the deficiency in compliance, the responsiveness of the financial institution to MAS' directions, and timeliness of their remedial actions. This achieves proportionality and effectiveness by targeting the identified root causes of the weakness in compliance. The sanctions that have been imposed and the basis for them are the following:-

- In the 12 cases where the institutions' AML/CFT framework and procedures met minimum requirements, but were not being effectively implemented due to resource constraints, MAS directed the institutions to increase their compliance resources within a specified timeframe.

- In another 2 cases where there were adequate AML/CFT framework and procedures but the root cause of inadequate implementation was assessed to be poor management commitment or ineffective management oversight, the senior management was replaced.

- In the 7 cases where the non-compliance was assessed to be due to deficiencies in the institution's AML/CFT framework and procedure, MAS directed the institution to conduct an independent review and undertake a remedial program, and to report back within specified intervals on the implementation of its remedial plans including in one case requiring independent verification of the remedial actions taken by the institution.

- In 2 cases, MAS had revoked the licences of the institutions. Both institutions were assessed to be lacking in commitment and resources to undertake the remedial actions needed, and had committed repeated breaches of the Notice.

583. There were no similar actions taken against insurance companies, as the deficiencies found were minor; however, they were always required to rectify the deficiencies noted within a reasonable time. With regard to Banks, Merchant Banks and Finance Companies, a total of 24 financial

institutions were involved, of which 11 had 2 or more actions taken against each of them. With regard to capital markets intermediaries and financial advisers, a total of 8 financial institutions were involved, of which 5 had 2 actions taken against them, and 1 had 4 actions taken against it.

584. Of the above-mentioned 92 fines imposed on holders of money-changer's or remittance business licences, 49 licensees had imposed for breach of the record keeping requirements under Section 16 of the MCRBA read with MAS Notice 3002 and section 10.2 of MAS Notice 3001, which obliges the licensee to implement the procedures, policies and controls that shall include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.

	2004	**2005**	**2006**	**2007 (as at 14 Nov.)**
Money changers	17	7	7	2
Remittance agents	11	4	1	0
Total	**28**	**11**	**8**	**2**
Total number of entities found to be in breach (2004 to 14 November 2007)	**49**			

585. Other weaknesses included insufficient training and controls. According to MAS, the licensees were fined for each instance of non-compliance with the requirements of the MCRBA and/or MAS Notices with SGD 250 to SGD 2 000. They also had to take remedial actions to prevent future lapses in internal controls. The enforcement actions taken in combination with stricter requirements for the annual renewal of the licence and the granting of new licences and enhanced training efforts have improved the AML/CFT compliance in this sector. A number of small operators decided to withdraw from the business.

586. To date, MAS has revoked the licenses of two remittance companies for several breaches of the MCRBA and licensing conditions including the failure to comply with CDD and record keeping requirements.

587. In imposing a sanction on a financial institution, MAS writes to the institution informing it of the specific AML/CFT Notice that had been breached and the grounds for MAS' finding, including forwarding a copy of the MAS inspection report with details of the nature of the deficiencies. The directions/reprimands are stated in mandatory terms, leaving no doubt that the institution has to comply with the terms of the sanction within the stated period.

588. There is also effective follow-up on the remedial actions. In every case, the institution is required to acknowledge the MAS letter and report, and revert with their remedial plans within four weeks, including details of the progress of implementation of those plans. Follow-up action is integral to the MAS overall supervisory approach - MAS inspectors are required (under the MAS Examination Manual and Guidance Notes on Supervisory Plan) when conducting annual risk review of financial institutions, to evaluate and account for the progress and effectiveness of remedial actions required to be taken from a previous inspection. MAS has therefore not experienced any instances where a financial institution refuses to comply with remedial actions as directed. In any case, any such refusal of a direction from MAS attracts criminal sanctions as described in R.17.

589. Given the criminal and range of administrative sanctions that are available, and have been applied for breaches in the AML/CFT Notices, the assessment team concluded that Singapore's AML/CFT sanctions regime is effective, proportionate and dissuasive. Follow-up actions to ensure that remedial steps are taken to help ensure effective implementation of the AML/CFT requirements.

Market entry – Recommendation 23

590. At the point of admission, financial institutions have to obtain MAS' approval to carry on business in Singapore. MAS' approval is generally required for: (1) the appointment of directors and senior management and in the case of institutions carrying out the banking business, nominating committees; and (2) specific threshold changes in shareholdings of the financial institution to ensure that criminals are prohibited from holding or controlling a significant investment in a financial institution, or from holding any management function in the financial institution. MAS' approval is also required for the appointment of senior management of the Singapore branches of financial institutions incorporated outside Singapore. Approval will only be given if MAS is satisfied that, inter alia, directors and senior management are fit and proper. For existing licensed financial institutions, MAS' approval is also required for the subsequent appointment of directors and senior management.

591. MAS' approval is also required for those who intend to hold or control a significant investment in a financial institution. At the point of admission, MAS will establish the identity of any person having the ultimate controlling interest or exercising controlling influence over the financial institution (beneficial owners). Again, approval will only be given if MAS is satisfied that, inter alia, such persons are fit and proper. The regulatory statutes governing each of the classes of financial entities require the approval of MAS if a person's shareholding in a financial institution crosses certain specified thresholds.[87]

Banking, securities and insurance sectors

592. The directors and some members of senior management of financial institutions that are subject to the Core Principles are required to satisfy the fit and proper criteria. This means that these appointment holders should have no criminal or other adverse regulatory records and have the qualifications and expertise appropriate for their level of responsibility. They are also expected to be financially sound. In addition, MAS requires that the relevant persons perform the regulated activities efficiently, honestly, fairly and act in the best interests of their customers/shareholders. However, the provisions providing for the fit and proper test are narrowly formulated and include only the directors, the chief executive officer and his deputy, the head of treasury, and the chief financial officer but not other senior managers (such as the compliance officer). The Singapore Authorities report that as a matter of routine, their supervision includes a control that the financial institution has ensured that the other members of senior management are fit and proper, and an assessment of the quality, competence and independence of the compliance function and that remedial measures are required where warranted.

593. In the process of approving the directors, senior management and beneficial owners of financial institutions, MAS checks with CRO and CPIB to ascertain if the applicants have any criminal records. MAS also checks the applicants' background against external commercially available databases. In addition, MAS will check with the home or host regulator (if they have worked overseas) to ensure that these persons have no criminal or other adverse records. Internal information is also used to check the background of the applicants.

594. MAS maintains internal records of information obtained in the course of its supervision of the financial institutions which pertains to the fitness and propriety of people in the financial sector.

[87] **Banks:** s.15A, 15B and 15C, Banking Act; Regulation 18, Banking (Corporate Governance) Regulations 2005; Notice 662A to Banks. **Finance companies:** s.10, 11, 12, Finance Companies Act; MAS Notice 817 to Finance Companies; **CMS licensees:** s.86 and 96, Securities and Futures Act; Regulation 12, Securities and Futures Act (Licensing and Business Conduct) Regulation 2002; Guidelines on Fit and Proper Criteria (MCG-G01). **Financial advisers:** s.9 and 56, Financial Advisers Act; Regulation 13 and 39, Financial Advisers Regulations 2002; Guidelines on Fit and Proper Criteria (MCG-G01). **Insurers:** s.27 – 29 and 31, Insurance Act; Guidelines on Fit and Proper Criteria (MCG-G01). **Money-changers and remitters:** s.7, 7A, 9A and 9B, MCRBA. **Trust companies:** s.5, 13 and 17, Trust Companies Act; Regulation 9, Trust Companies Regulations 2005. **Approved trustees:** s.287, Securities and Futures Act.

Where the situation calls for it, MAS will conduct insolvency screening as well as request the applicant to provide a credit bureau search report.

Financial institutions other than banks, securities, and insurance

595. In Singapore, the following types of financial institutions are not subject to the Core Principles:

(a) Money-changing or remittance business licensees, approved trustees and trust companies. These financial institutions are required to be licensed and registered (s.5 and 6, MCRBA; s.289, Securities and Futures Act; s.3, Trust Companies Act).

(b) Moneylenders and commodity futures brokers.

596. Moneylenders are regulated under the Moneylenders Act that comes under the purview of the Ministry of Law. They need a licence to carry on their business (s.5 and 8 Moneylenders Act). Under new Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2007 issued on 12 November 2007, they are now also subject to supervision and oversight for AML/CFT purposes.

597. Commodity futures brokers are regulated under the Commodity Trading Act and need a licence under section 12 of the Act to carry on their business. From February 2008 on, these brokers will have their licences transferred to a Capital Market Services licence under the Securities and Futures Act and will then need to comply with the relevant MAS AML/CFT Notice. At the date of the on-site visit they were not subject to supervision and oversight for AML/CFT purposes.

598. No person (natural or legal person) shall carry on a money-changing or remittance (value transfer) business unless he is in possession of a valid money-changer's or remittance business' licence respectively. Any person who contravenes sections 5 or 6 of the MCRBA shall be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD 100 000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a fine not exceeding SGD 10 000 for every day during which the offence continues after conviction. Unlike other financial institutions regulated by MAS, the licences of all money changers and remittance agents are renewable annually. MAS may refuse to renew their licences if they do not comply with the AML/CFT requirements and such breaches are sufficiently serious to warrant a strong regulatory action.

599. As detailed in the licensing/registration application forms (which are available on the MAS public website), checks are made on the money-changing or remittance business licensees, approved trustees and trust companies to ascertain whether they, the directors and senior management are fit and proper. Areas which are checked include:

(a) Whether the individual has been convicted of any offence in Singapore or elsewhere or been subject to any proceedings currently pending which may lead to such a conviction.

(b) Whether any judgment (including a finding of fraud, misrepresentation, or dishonesty) has been given against him in any civil proceedings in Singapore or elsewhere.

(c) Whether the individual has been declared bankrupt or compounded with or made an assignment for the benefit of his creditors in Singapore or elsewhere.

(d) Whether he has been refused the right or restricted in his right to carry on any trade, business or profession in any jurisdiction.

600. The executives of these financial institutions must pass screening tests with entities like CPIB and CRO. MAS also carries out insolvency checks and background checks on such individuals against an internal database.

601. Although MAS has the power (.18 MCRBA) to authorise a person to enter and inspect the premises, where according to its knowledge or suspicion the carrying on of an unlicensed money-changing or remittance business takes place, it has not used this power to date. Such cases were rather referred to CAD for investigation. Allegations of unlicensed business could arise with CAD through referrals from MAS, alerts of industry competitors, anonymous complaints, and STRs. During the investigation the police will work closely with MAS to determine the status of the business under investigation. The range of punishment is between SGD 5 000 and 50 000. In one case the accused was sentenced to a fine of SGD 50 000 and a term of imprisonment of 2 weeks

Prosecution and conviction for unlicensed remittance/money-changing business

Prosecution and conviction for unlicensed:	2004	2005	2006	2007 (as at 14 November)
• Remittance businesses	4	5	2	-
• Money-changing	1	3	1	2 + 2*

*The two cases have been recommended for prosecution under the MCRBA.

Ongoing supervision and monitoring – Recommendation 23

Banking, securities and insurance sectors

602. For financial institutions that are subject to the Core Principles (*i.e.* banks, merchant banks, finance companies, financial advisers, CMS licensees and insurers), MAS applies similar supervisory measures used for prudential purposes in relation to AML/CFT. MAS views ML/FT risks with equal importance as other risks faced by the financial institutions, such as credit, market and liquidity risks.

603. **Licensing and structure:** In the admission of financial institutions, MAS takes into account both quantitative and qualitative factors. Apart from meeting the quantitative criteria such as financial strength and credit ratings, MAS would consider qualitative factors such as the applicant's home country's compliance with FATF standards and the quality of home country supervision over the foreign financial institutions' branches and subsidiaries. The adequacy of the financial institution's AML/CFT policies, procedures and controls, its reputation, as well as its compliance track records (*i.e.* whether the financial institution has been the subject of regulatory action for AML/CFT breaches) are also important considerations in processing the application for a licence.

604. **Risk management**: MAS will request for information on the applicant's risk management framework and exposures at the point of admission. For financial institutions operating in Singapore, MAS holds the Board and senior management responsible for ensuring that the financial institution has an adequate risk management framework and procedures to identify, measure, monitor and control material risks, which include money laundering and terrorist financing risks.

605. **Consolidated Supervision** Consolidated supervision as required by the Core Principles applies to banks and insurers. In the course of inspecting local financial institutions, MAS assesses the oversight of the head office on the AML/CFT aspects of their overseas branches and subsidiaries and compliance with the MAS Notices. MAS conduct periodic inspections on the overseas branches or subsidiaries of its locally incorporated banks depending on their significance to the financial institution's overall operations. See section 3.8 of this report for more details relating to the supervision of foreign branches/subsidiaries of financial institutions.

606. **Ongoing supervision:** During the inspection of financial institutions, MAS examiners will review the roles, responsibilities and extent of commitment of the Board and senior management in preventing ML/FT. MAS further reviews the involvement of the Board and senior management in setting policy direction on AML/CFT and the processes by which they are kept informed of risk

management efforts, deficiencies and corrective actions taken in relation to preventing money laundering. The financial institutions will also be assessed on whether appropriate risk management strategies are adopted, approved by the Board, and whether policies and procedures (including ongoing employee training programme, internal audit, compliance and risk management functions) relating to anti-money laundering and counter-terrorist financing measures are properly documented, reviewed, updated and communicated within the financial institution, and adhered to in practice by performing sample testing of transactions. MAS also tests the effectiveness of the systems put in place by the financial institutions.

607. If it is assessed that the risk management processes are inadequate for the size and nature of the activities of the financial institution, MAS will require the financial institution to take corrective actions to strengthen its risk management processes. All significant examination findings will be sent to the Board and/or senior management to ensure that the financial institution rectifies the weaknesses highlighted.

608. MAS monitors the statistics of the suspicious transaction reports submitted by the financial institutions to STRO. The suspicious transaction reports, that are copied to MAS, are reviewed by MAS to see if there are control deficiencies relating to the prevention of ML/FT, and if so, MAS will follow up with the financial institutions concerned accordingly. MAS examiners assess the system put in place by the financial institutions to monitor transactions, review transaction monitoring reports as well as the escalation process for STRs. To identify and detect suspicious transactions, institutions are expected to assess whether a particular transaction is suspicious, in relation to their knowledge of the customer's profile and transaction history. Institutions must consider the totality of the transactions put together and not each transaction (which, on its own, may be perfectly legitimate) in isolation. For transactions which may appear suspicious initially but did not warrant the filing of any STR eventually, MAS examiners will evaluate the analyses done by the financial institutions and the comprehensiveness of documentation and record keeping. In cases where a suspicious transaction may not have been reported or where deficiencies in CDD procedures, transactions monitoring or other requirements spelt out in the MAS Notices exist, MAS would highlight these deficiencies as a non-compliance with the MAS Notices and require the financial institutions to take prompt remedial actions.

609. In addition, MAS keeps track of AML/CFT related news involving financial institutions that have a presence in Singapore. For example, if a financial institution is reported to have been issued a regulatory order by other supervisory authorities, MAS will follow up with the Singapore branch/entity to ensure that similar deficiencies or weaknesses do not exist there.

610. MAS conducts both routine and thematic on-site inspections of the financial institutions under its supervision. The scope and frequency of inspection varies among the financial institutions, depending on MAS' impact and risk assessment on the financial institutions. An outline of the features of the Common Risk Assessment Framework and Techniques (CRAFT) is set out above. All financial institutions are subjected to base-level supervision and monitoring, with increased supervisory attention given to the financial institutions with high risk and impact ratings. Financial institutions deemed to have higher AML/CFT risks based on their activities, customer base, products/services offered and geographical locations would be subject to more frequent inspections. The inspection period for each financial institution could range from 2-3 days for institutions like financial advisers to 1-4 weeks for banks, depending on the size of the financial institution and the scope of inspection.

Overview of inspections/supervisory visits that included AML/CFT

	2004	2005	2006	2007 (as at 14 Nov.)
Banks and Merchant Banks	27	41	25	27
Remittance Agent	12	6	3	4
Money Changer	20	8	7	4

	2004	2005	2006	2007 (as at 14 Nov.)
Capital Markets Services Licensees	48	56	34	14
Licensed Financial Advisers	-	-	6	-
Approved Trustees	-	-	-	-
Trust Companies	-	-	-	5
Insurance Companies	2	1	4	6
Grand Total	**109**	**112**	**79**	**60**

611. As part of the above mentioned numbers of the inspections and supervisory visits, MAS carried out the following number of "thematic" AML/CFT inspections, *i.e.* inspections that targeted only AML/CFT areas.

	2004	2005	2006	2007 (as at 14 Nov.)
1) Banks, Merchant Banks, Finance Companies	-	15	-	5
2) Capital Markets Intermediaries, Financial Advisers, Trust Companies, Approved Trustees	-	-	31	5
3) Life Insurance Companies	-	-	-	5

612. MAS reviewed the adequacy of the AML/CFT policies, procedures and controls of the inspected institutions as well as their compliance with MAS' regulations. MAS conducted sample testing of transactions in all inspections. In summary, some of the common weaknesses noted included:

(a) Inadequate policies and procedures.

(b) Deficiencies in CDD.

(c) Weaknesses in transaction monitoring systems.

(d) Insufficient training.

613. In addition, MAS required the appointment of independent external auditors for four Capital Market Services licensees. For Capital Market Services licensees not covered under the 2006 AML/CFT thematic inspections, MAS sent them the self assessment questionnaire for the purposes of the offsite review

Financial institutions other than banks, securities, and insurance

614. Money lenders were issued with AML/CFT rules by the Ministry of Law on 12 November 2007 and will be supervised for their compliance with them. [88]

[88] The AML/CFT legislation is still new and the Registrar will require time in gathering feedback, to consult with various participants and to acquire the necessary experience in order to enable him to formulate policies and further activities in the programme of supervision. However, the authorities have indicated that the Registrar intends to take a multi-pronged approach to supervising compliance by moneylenders, which includes incorporating such compliance in the Registry's inspections of moneylenders, issuing guidelines to moneylenders to assist them in their compliance, and disseminating information from time to time on the latest developments, trends and typologies.

615. Commodity futures brokers will have their licences under the Commodity Trading Act transferred to a Capital Market Services licence under the Securities and Futures Act in February 2008 and will then need to comply with the MAS AML/CFT Notice´SFA04-N02. As a result of this timing, the substantive assessment of compliance with these obligations (including the rating) does not take these new requirements into account. At the date of the on-site visit they were not subject to supervision for AML/CFT purposes.

616. All money-changing or remittance business licensees, approved trustees and trust companies are subject to AML/CFT requirements under MAS AML/CFT Notices and are subject to MAS' oversight. They are also subject to the provisions of the CDSA and TSOFA. Additionally, money-changing and remittance business licensees are required to comply with the:

(a) Money-changing and Remittance Businesses Act.

(b) MAS Notices to Holders of Money-changer's Licence and Remittance Licence.

(c) Money-changing and Remittance Businesses Regulations 2005.

(d) The Monetary Authority of Singapore (Anti-Terrorism Measures) Regulations 2002.

617. MAS monitors the regulatory compliance of all money-changing and remittance businesses licensees through onsite and offsite supervisions. Licensees are required to submit returns and information on their operations / transactions (s.17 - 18, MCRBA). MAS may also require the external auditor of a money-changing or remittance business licensee to submit an auditor's report (s.26(2d), MCRBA).

Guidelines – R.25 (Guidance for financial institutions other than on STRs)

618. MAS, as the regulator for the financial sector, has issued various notices on AML/CFT requirements. These Notices on Prevention of Money Laundering and Countering Terrorist Financing, which are complemented by guidelines, serve to assist financial institutions in understanding their AML/CFT obligations. Contained within the Guidelines is information regarding the manner of reporting, the specific reporting form to use and the procedures that should be followed when reporting an STR. The list of guidelines include:

S/No.	Description	Sector	Relevant Authority
1	Guidelines to MAS Notice 626	Banks	MAS
2	Guidelines to MAS Notice 1014	Merchant Banks	
3	Guidelines to MAS Notice 3001	Money-Changers and Remittance Agents	
4	Guidelines to MAS Notice 824	Finance Companies	
5	Guidelines to MAS Notice 314	Insurance	
6	Guidelines to MAS Notice FAA-N06	Financial Advisers	
7	Guidelines to MAS Notice SFA04-N02	Capital Markets Services Licensees and Exempt Persons	
8	Guidelines to MAS Notice SFA13-N01	Approved Trustees	
9	Guidelines to MAS Notice TCA-N03	Trust Companies	

619. In July 2007, MAS circulated to financial institutions the Guidance for Implementing a Risk Based Approach to Combating Money Laundering and Terrorist Financing approved by the FATF Plenary in June 2007.

620. CAD and STRO organise periodic outreach sessions geared to various classes of the financial sector and to DNFBPs to raise the awareness of the basic concepts of ML and TF, of the STR obligations under the provisions of the CDSA and TSOFA and other measures to be put in place such as CDD and sound internal controls. For the same purpose and to account for its work, STRO also publishes periodically the Reports from STRO. In its outreach programs to financial institutions, CAD uses the MAS Notices to provide guidance on effective AML/CFT measures. CAD has published the 2nd edition

of AML/CFT Handbook and a 3rd edition is in the pipeline. In addition, STRO is developing its own internal set of guidelines to educate the general public on AML/CFT measures and knowledge.

Statistics and effectiveness

621. MAS maintains statistics on the on-site examinations of financial institutions that include AML/CFT as well as sanctions applied. Singapore has subjected a wide range of financial institutions to adequate AML/CFT regulation and supervision. However, commodity futures brokers will only come under an AML/CFT regulation in February 2008 and moneylenders have only been issued with AML/CFT regulations in November of 2007 and the effectiveness of their implementation has yet to be tested. Within the main financial sectors (banking, insurance, securities, etc.), the team notes that there is a strong compliance culture throughout. Additionally, MAS can publish letters of reprimand on its public website, giving financial institutions a strong incentive to comply, for fear of reputational risk.

622. In recent years, MAS supervision has focused particularly on an adequate and effective AML/CFT regulation and implementation. MAS relies on extensive on-site inspections and on policy, implementation and effectiveness discussions with management and head compliance. MAS applies a wide range of sanctions. The policy to ask for remedial actions and follow up on the progress seems to be effective, not least in view of the stringent enforcement policy of MAS.

3.10.2 Recommendations and Comments

623. Sectors not yet covered for AML/CFT (commodities future brokers) should be covered as soon as possible.

624. In some cases, (*e.g.* for banks, but also for some other classes of financial institutions), the fit and proper test is applied to a limited circle of persons, such as the directors, the chief executive officer and his deputy, the head of treasury, and the chief financial officer; Singapore should extend the fit and proper test to all senior management.

625. Singapore has large communities of migrant workers from countries with poor banking systems. MAS has adopted various measures to encourage the public to remit money via formal channels (encouraging banks to set up specific-purpose remittance branches; granting remittance licences to subsidiaries of foreign banks so that nationals of the banks home country working in Singapore have alternatives to banks for remitting funds; educating foreign workers through brochures to be more discerning in their choice of remittance channels). Nonetheless, Singapore should also develop more pro-active policies for assessing the risk of the unlicensed remittance sector with a view to reducing the number of possible money-changing and remittance businesses.

3.10.3 Compliance with Recommendations 23, 29, 17, & 25

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17	**LC**	• Effective, proportionate, and dissuasive sanctions for non-compliance with AML/CFT obligations do not yet apply for commodity futures brokers, and the effectiveness of the sanctions for money lenders has not yet been tested.
R.23	**LC**	• Commodity futures brokers are not yet supervised for AML/CFT, and the effectiveness of the supervisory regime for money lenders has not yet been tested. • Fit and proper tests do not apply to all senior management. • The risk of unlicensed MVTs is not adequately addressed.
R.25	**LC**	• (Compliant with respect to financial institutions. Guidelines have to be issued to a number of DNFBPs.)
R.29	**LC**	• There are not AML/CFT inspection and enforcement powers for commodities future brokers. • As the provisions that apply to moneylenders are very recent , it is not yet possible to assess their effectiveness.

3.11 Money or Value Transfer Services (SR.VI)

3.11.1 Description and Analysis

626. In Singapore, money-changing or remittance businesses are regulated under the MCRBA that come under the purview of MAS. They need a licence to carry on their business (see section 3.10 of this report for more details on licensing requirements) and are subject to MAS Notices including the MAS AML/CFT Notice. Their license has to be renewed annually. MAS maintains a database of the names and addresses of licensed money-changers and remittance agents, their directors, shareholders and their shareholdings, and updates the database regularly for any changes. All money remittance agents must also be licensed directly by MAS. MAS' policy is that remittance agents are licensed primarily to provide remittance services to customers residing in Singapore. In the event that licensees also provide remittance services to facilitate fund transfers between foreign parties in different countries, they could be directed to cease such transactions if they are deemed to pose high ML/FT risks.

627. The Singapore authorities have made some efforts to locate unlicensed remitters and sanction them accordingly. MAS has the power (s.18, MCRBA) to authorise a person to enter and inspect the premises, where according to its knowledge or suspicion the carrying on of an unlicensed money-changing or remittance business takes place; however it has not used this power to date. Such cases were rather referred to CAD for investigation. Referral of unlicensed businesses to CAD is usually for the purpose of prosecuting and convicting the unlicensed remitters. Allegations of unlicensed business could arise with CAD through referrals from MAS, alerts of industry competitors, walk-in or anonymous complaints, and STRs. During its investigations, the police will work closely with MAS to verify the status of the remittance business and in particular, whether a valid license has been issued.

628. Between 2004 and 31 July 2007, the police have successfully prosecuted and secured a conviction in 18 cases of unlicensed remittance/money-changing businesses. Another three cases were under investigation at the time of the on-site visit. The punishments in these cases ranged from a fine of SGD 5 000 to the maximum of SGD 50 000. In one case, the accused was sentenced to a fine of SGD 50 000 as well as a term of imprisonment for 2 weeks. The following is a breakdown of the statistics for the prosecution and conviction results on unlicensed remittance business received by the Police:

Prosecution and conviction for unlicensed remittance

Prosecution and conviction for unlicensed	2004	2005	2006	2007 (as at 14 Nov.)
• Remittance businesses	4	5	2	-

629. Apart from carrying out enforcement actions against unlicensed remittance agents/money changers, the police also conduct public outreach to members of the public to educate them of their obligations when conducting a remittance/money-changing business. Examples of this outreach include the joint outreach with the Moneychanger Association (which includes remittance businesses) and STRO in February and August 2007.

630. All money-changing and remittance business licensees are required to comply with MAS Notice 3001 and the accompanying Guidelines, which relate to the implementation of the FATF Recommendations. The deficiencies described elsewhere with respect to Rec. 4-11, 13-15, 21 and 23 (CDD, record keeping, STR reporting, tipping off, etc.) as well as wire transfer apply equally to MVT operators.

631. MAS examiners will check if licensees comply with AML/CFT requirements during onsite inspections. For a detailed description of the MAS supervisory system, see section 3.10 of this report. The licensees may have to submit annually an auditor's report. In this report, the auditor has to confirm that there has been no contravention by the licensee of any conditions, restrictions, obligations or other requirements provided under, among others, the applicable MAS AML/CFT Notice, the CDSA, the TSOFA and the MCRBA. In addition, the licence has to be renewed annually.

632. As money changing and remittance business licensees are licensed and supervised by MAS under the MCRBA, all licensees are subject to the range of sanctions as set out in section 3.10 of this report for failure to comply with AML/CFT requirements. A number of money changing and remittance businesses have been fined and two (as of 14 November 2007) have had their licences revoked.

Statistics and effectiveness

633. Over the last years the conditions for granting a new or renewing an existing licence have been made more stringent. This has lead to some structural reforms in the sector. A number of smaller businesses have renounced their licences. MAS applies the same policies of inspection and remedial action as it applies to other financial institutions; however, it applies more often pecuniary sanctions to MVTs and money-changing businesses.

634. During the time of the on-site visit, the assessment team had some doubts about the legal authority to inspect and obtain information from money remittance companies for AML/CFT breaches in limited circumstances. However, MAS has imposed additional licensing conditions on all licensees on 8 October 2007 which explicitly provide for MAS' inspection of these sectors and the requirement to furnish information for the purpose of assisting MAS in monitoring the licensees' level of compliance with the relevant MAS AML/CFT Notices.

635. Singapore hosts a high number of migrant workers from countries with poorly developed banking systems. It is to be expected that they use extensively alternative remittance systems to transfer money to their families. This suggests that Singapore might have an elevated risk of unlicensed MVT businesses. However, Singapore has not sufficiently studied the extent of this risk and developed pro-active policies to curb it. Singapore is, however acting against unlicensed MVTs, albeit mostly through the police rather than the financial market supervisor.

3.11.2 Recommendations and Comments

636. Singapore has broadly implemented the requirements in SR.VI through licensing requirements, inspections for compliance with those requirements, and appropriate sanctions. However, Singapore should develop more pro-active policies with a view to reducing the number of possible unlicensed money-changing and remittance businesses considering the large communities of migrant workers from countries with poor banking systems present in Singapore.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**LC**	• The risk of unlicensed MVTs is not fully addressed. • The limitations identified under Recommendation 5, 8, 10, 13, 14 and SR.VII also affect compliance with Special Recommendation VI.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPS)

General Description

637. Singapore has applied AML/CFT preventive measures to trust companies (that are regulated as financial institutions) and lawyers. Singapore has not yet applied preventive measures to accountants when they undertake the type of work covered by Recommendation 12, trust service providers (other than trust companies and lawyers), company service providers, dealers in precious metals and stones and real estate agents. Physical casinos are not in operation yet. All DNFBPs are bound by the CDSA provisions on suspicious transaction reporting (s.39), tipping off (s.48) and protection from liability (s.39(6), as described in section 3.6 and 4.2 of this report.

638. **Physical casinos** will be opened for the first time in Singapore in 2009. In light of this, a Casino Control Act (CCA) was passed in February 2006. AML Regulations are expected to be issued pursuant to Section 200(2) of the CCA, and to apply to both the casino operators and junket promoters[89].

639. **Internet casinos** are prohibited from being set up in Singapore under the Common Gaming Houses Act. Service providers in Singapore (like payment gateway providers) could be prosecuted for an offence under the Common Gaming House Act when they knowingly provide services that would in any way assist an Internet gambling website. Therefore, banks in Singapore block credit card payments to internet casinos with the help of the credit card companies.

640. **Real estate agents** in Singapore usually do not play any role in the legal or financial aspects of real estate transactions. However, there is no legal prohibition for real estate agents to handle the financial aspects of a real estate transaction. In practice, the "gatekeeping" function for real estate transactions is assumed by lawyers who are expressly subjected to AML/CFT regulations. Real estate agents' role is to market the property. They assist the purchaser to find the right property at the right price, guide the client through the process, make sure all pre-purchase issues are properly covered and make recommendations on financing and legal representation. Once the option money of usually 1% of the purchase price is handed over and the purchase option thus secured, a lawyer is appointed and assists the purchaser with the transaction, and in particular with the financial and legal aspects of it. Real estate transactions that involve estate agents and not lawyers number less than ten per year and are considered so unusual that, according to Singapore authorities, they are immediately noticed by the Singapore Land Authority which will automatically file an STR with the STRO (the FIU).

641. **Dealers in precious metals and dealers in precious stones**: Singapore does not regulate dealers in precious metals and dealers in precious stones. A large number of them are member of the Singapore Jewellers Association which is, however, not a self-regulatory organisation with mandatory membership.

642. **Lawyers** are regulated under the Legal Profession Act and Rules made pursuant to that Act, including the Legal Profession (Professional Conduct) Rules ("the Rules"). In the context of real estate transactions, lawyers are responsible for drawing up of the sale and purchase agreement, and registering the interest in and transfer of title to the property with a central government land registry, the Singapore Land Authority. Lawyers are also involved in the payment of a deposit (that accompanies the execution of a sale and purchase agreement) and full payment of the purchase price upon completion of the transaction.

643. **Notaries**. The functions that notaries perform correspond generally to those performed by notaries in the United Kingdom and encompass the powers and duty to attest deeds, contracts, and other instruments that are to be used abroad and to give a certificate of the due execution of such documents duly authenticated by the notary's signature and notarial seal. They also draw up certain documents such as Ships' Protests, and protest Bills of Exchange. Only practising advocates and solicitors of Singapore that have been practicing for not less than 7 years are eligible to be appointed as a notary public. Accordingly, notaries do not perform in the course of their incidental work the activities which are subject to the FATF Recommendations.

644. **Accountants:** The accountancy profession in Singapore comprises roughly 18 000 practitioners. Public Accountants (auditors) are regulated under the Accountants Act and regulations. The Institute of Certified Public Accountants of Singapore (ICPAS) is the national organisation of the accountancy profession in Singapore. ICPAS issues guidance to its members. Although membership is not mandatory, most auditors and industry practitioners are members. A

[89] Plans are to put in place KYC, CDD measures such as the identification of customers, verification of identity and ongoing monitoring. The identification of customers shall include, but will not be limited to, their full names, unique identification numbers, existing residential address, date of birth, nationality, etc.

distinction is made between practising members (members in the auditing profession, about 800) and non-practicing as well as provisional members working in audit firms, commerce and industry. Other persons calling themselves “accountants” and performing general accounting activities are not regulated.

645. **Trust service providers.** The First Schedule of the Trust Companies Act defines the trust business to encompass the following activities:

(a) Provision of services with respect to the creation of an express trust.

(b) Acting as trustee in relation to an express trust.

(c) Arranging for any person to act as trustee in respect of an express trust. Or

(d) Provision of trust administration services in relation to an express trust.

In addition, the MAS Guidelines on Scope of Regulation (TCA-G04 of 22 December 2005) specify in more details what activities are covered by the First Schedule.

646. Whoever carries on any “trust business” in or from within Singapore has to be licensed as a trust company. Trust companies are defined as financial institution and regulated by MAS under the Trust Companies Act (TCA). The AML/CFT requirements that apply to trust companies are described in detail in section 3 of this report.

647. The Act provides for two types of exceptions from the licensing principle. First, under s.3(3) and the Second Schedule to the TCA, persons engaging in certain types of activities are exempt from the licensing requirement, namely the bare trustee, the trustee or administrator of a business trust, the trustee-manager of a registered business trust, a person preparing or advising on a will and a person acting as the executor or administrator of the estate of a deceased person

648. Second, under s.15(1) of the Act, certain persons or classes of persons are exempt from the licensing requirement when providing trust services, among them banks, merchant banks and holders of a capital market services licence and such other person or class of persons as may be prescribed. Such prescription has been made through the Trust Companies (Exemption) Regulations 2005, that exempts among others lawyers and law practices approved or registered under the Legal Profession Act and public accountants and accounting corporations registered or approved under the Accountants Act. For most classes, the nature of the exempt service(s) is set out in the Exemption Regulations. One part of the so exempt services for lawyers and law practices is subject to limitations as to the amount (not more than SGD 2 million, excluding real property) settled in one or more trusts by a client, and number of clients per lawyer (not more than 30) and to certain reporting requirements (s.4(1)(b)(iv) and s.5(4) and (5). With the necessary modifications (s.5 Exemption Regulations), exempt persons under the Exemption Regulations are subject to the inspection and investigative powers of the Trust Company Act (ss.40-46); the sections on falsification of records by officer, auditor, employee or agent of licensed trust company (s.61); the duty not to furnish false information to an authority (s.62); as well as to the regulation on advertisement (regulation 16 of the Trust Companies Regulations 2005).

649. For ease of reference throughout this section, unless otherwise specified, the term Trust Service Provider is used only to refer to the activities of trust service providers where that activity is not carried out by a licensed trust company.

650. **Company service providers**: Singapore regulates company service providers. These providers are authorized to represent companies and other business entities upon satisfaction of certain criteria. Only "prescribed persons" (under the Business Registration Act, the Companies Act, and the Limited Liability Partnerships Act) may file documents on behalf of a third party. The list of prescribed persons includes advocates and solicitors, accountants registered with the Institute of Certified Public Accountants of Singapore, a member of the Singapore Association of the Institute of Chartered Secretaries and Administrators, a corporate secretarial agent, and members of other prescribed professional associations (s.12A, CA; s.42, LLP; s.20, BR Act).

4.1 Customer Due Diligence and Record-Keeping (R.12)

(Applying R.5, 6, and 8 to 11)

4.1.1 Description and Analysis

651. The FATF Recommendations do not apply to auditing activity. Nevertheless, Singapore has issued some AML/CFT guidance to auditors (SAP 19). While it is not clear whether this guidance applies to the non-auditing activities of auditors, it is not enforceable in any event.

Applying Recommendation 5 (CDD)

652. Currently, requirements to apply customer due diligence (CDD) in accordance with Recommendations 5 have only been issued for lawyers. Trust Companies are regulated as financial institutions; see section 3 for a description of how trust companies must apply CDD.

Applying Recommendation 5 (Accountants)

653. ICPAS has issued a Revised Statement of Auditing Practice (SAP 19) on Guidance to Auditors on Money Laundering and Terrorist Financing. The stated purpose of the SAP is to provide auditors with updated information about current AML/CFT legislation, guidance on compliance with it and guidance to auditors as to their responsibilities on auditing and reporting on financial statements. In this context, SAP 19 contains certain provisions on KYC and documentation. However, the guidance on these issues is general, broad and focussed on how they apply to an auditing context.

654. SAP 19 states that when other services (such as giving advice or administrative services in the ordering of personal affairs; advising on the setting up of trusts, companies or other bodies; arranging loans; acting as a trustee, nominee or company director) are provided, *"...the procedures undertaken in the provision of those services may facilitate judgments 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"* (s.14).Section 11 indicates that the SAP *"gives guidance concerning the effects of AML and ATF legislation on the work undertaken in relation to reporting on financial statements of entities...., including the auditor's statutory reporting duties"*. It is not clear if the reference to the similar application of the guidance is only to the guidance concerning the reporting obligations or also to the guidance on other subjects such as KYC or documentation. Arguably the last sentence of section 14 refers to the guidance of the SAP on the reporting obligation only. Furthermore, SAP 19 does not have the status of other "enforceable means" in a non-auditing context.

Applying Recommendation 5 (Lawyers)

655. Lawyers are subject to the Legal Profession (Professional Conduct) Rules (the 'Rules') issued by the Law Society. Amendments to the Rules with respect to CDD and record keeping came into operation on 15 August 2007. The Rules have the force of law as secondary legislation under the Legal Profession Act and are enforced by the Law Society of Singapore. Breach of the Rules will lead to disciplinary proceedings against the lawyer concerned, pursuant to section 83, which may result in the offender either being struck off the roll, suspended from practice, censored, or ordered by the Council of the Law Society to pay a penalty or be reprimanded (s.88 and 94 Legal Profession Act).

656. The Council of the Law Society has also issued a Practice Direction on AML/CFT that came into force on 15 August 2007. It sets out more details and complements the obligations under the Rules. The Practice Direction replaced the previously applicable "Guidelines on the prevention of money laundering and the funding of terrorist activities" of 1 March 2003. Practice Directions are not subsidiary legislation (*i.e.* regulation). However, they are enforceable means as anyone found guilty of a breach of any usage or rule of conduct (which includes breach of a Practice Direction) made by the Council that amounts to improper conduct will face disciplinary proceedings under section 83(2)(b) of the Legal Profession Act. The authority of the Council of the Law Society to issue and enforce

Practice Directions has been confirmed by case law.[90] Rule 11D and the relevant provisions of the Practice Direction on KYC requirements apply to all transactions handled by lawyers, not merely to the 5 types of transactions listed in Recommendation 12.

Anonymous accounts

657. The Rules provide that lawyers shall not open or maintain any account for or hold and receive moneys from any anonymous source or a client with an obviously fictitious name (the Rules, Rule 11E; Practice Direction, (H)(5).

When CDD is required

658. The Rules require lawyers or law practices to take reasonable measures to ascertain the identity of a client as soon as reasonably practicable before accepting instructions to act in any matter (Rule 11D). This would presumably include when establishing business relations or conducting an occasional transaction on behalf of the client. The scope of the PD (PD(A)(6)) states that the directions are meant to apply whenever there is suspicion of the law practice being used for ML/FT or whenever the lawyer has "doubts about source of funds of their client or veracity/adequacy of identification data given the client or… information given to the law practice for transactions especially when instructed to establish business relations or carry out an occasional transaction." There is, however, no specific requirement to conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Required CDD measures

659. Rule 11D contains the general requirement to "take reasonable measures to ascertain the identity of a client,…the principal client,…[and] the natural persons that have a controlling interest in or that exercise effective control over the client". No further details are contained in law or regulation. However, the Practice Direction (which is other enforceable means) sets out the following elaboration.

660. ***Natural persons:*** The Practice Direction requires lawyers to obtain the following customer identification information:

- Full name (including all aliases).
- Date of birth.
- Nationality.
- Identity card number or passport number.
- Residential address.
- Occupation and identity and address of employer or, if self-employed, the name and place of the client's business (only if necessary).

661. For verification purposes, reliable, independent data/information is required to be obtained (Rule 11D; Practice Direction, (C)(II)(a – b).

662. ***Legal persons:*** The Practice Direction requires lawyers to verify the legal status of customers who are not natural persons. For corporate entities, lawyers are required to obtain a copy of the corporation certification. For partnerships and limited liability partnerships, the identity of each partner must be adequately verified. (Practice Direction, (C)(III)(2 - 4); Practice Direction, (C)(II)(c). For

[90] In the case of "The Law Society of Singapore v Disciplinary Committee" [2000] 4 SLR 413 before the High Court, although the solicitors were acquitted of improper conduct on the facts of that particular case, the High Court did not doubt that the Council had the power to enact and enforce the relevant Practice Directions of the Council (dated 20 May 1996).

charities, clubs and societies they are required to check with the Charity Commissioner or Registrar of Societies (where applicable) that the registration number of the organisation is correct. A copy of the constitution or trust deed, of the charity or society must be obtained by the lawyer. For co-operatives, the registration particulars of the cooperative have to be checked and a copy of the by laws of the society have to be obtained. For estates, lawyers are required to see the death certificate, original Will or a certified true copy of the Will of the deceased (where applicable) and obtain the relevant documents to ascertain the identities of the executors or administrators to the estate (Practice Direction, (III)(2 – 9). Rule 23 requires lawyers to ensure that an agent giving instructions on behalf of a client has the required authority to do so. In the absence of evidence of such authority, the lawyer must confirm the instructions with the client (see further elaboration of these requirements in Practice Direction, (C)(11)(a) and (c).Paragraph C III (2) of the Practice Direction further states, for avoidance of any possible doubt, that in relation to corporate clients, the "lawyer/ law practice must… ascertain the identity and particulars of the person who purports to instruct him on behalf of the corporate client."

663. ***Legal arrangements:*** With respect to trusts, the Practice Direction requires lawyers to ascertain the identity and particulars of each trustee, the nature of the trust and the identity of each principal beneficiary of the trust.

664. ***Beneficial ownership:*** There is no specific requirement for lawyers to identify the "beneficial owner" for all customers, although for those that are not natural persons reasonable measures must be taken to ascertain the identities of the natural persons that have a controlling interest in or exercise effective control over the client (Rule 11D and Practice Direction (C)(II)(d)). Also, the identities of all beneficial owners of a trust have to be established (Practice Direction (C)(II)(c)). Rule 11D also requires lawyers to take reasonable measures to ascertain the identity of the principal client before accepting instructions to act, which seems to impose a duty on the lawyer to inquire as to whether the client is acting on behalf of another person (i.e. a principal). For a body corporate, an unincorporated entity or an estate, lawyers are required to identify the relevant directors, partners, trustees, officers, members of committee of management or executors or administrators in those bodies respectively. These include corporations, partnerships and limited liability partnerships, trusts, charities, clubs, societies, co-operatives, management corporations and estates (Practice Direction, (III)(2 – 9). Lawyers are also required to obtain a list of shareholders of the company. However, there is no specific requirement to understand the ownership and control structure of the customer.

665. ***Purpose of the business relationship:*** Rule 11F provides that lawyers must obtain satisfactory evidence as to the nature and purpose of the business relationship with the client and the business relationship between the client and any other party to the matter, when acting on behalf of a client on any of the following matters:

- Acquisition, divestment or any other dealing of any interest in real estate.
- Management of client's moneys, securities or other assets, or bank, savings or securities accounts.
- Creation, operation or management of a company, corporation, partnership, society, trust or other legal entity or legal arrangement.
- Acquisition, merger, sale or disposal of a company, corporation, partnership, business trust, sole proprietorship or other business entity. Or,
- A matter that is unusual in the ordinary course of business having regard to:

    (i) The complexity of the matter.

    (ii) The quantum involved.

    (iii) Any apparent economic or lawful purpose of the matter.

    (iv) The business and risk profile of the client.

666. However, this would not seem to extend to situations in which the lawyer is organising contributions for the creation, operation or management of companies, as is required by the FATF Recommendations.

667. Practice Direction (D)(1 - 11) elaborates on Rule 11F, requiring lawyers to take a broad view of the term "business relationships". The Practice Direction sets out directions for each of the transactions listed above, *e.g.* red flags for land transactions (para. 6) and information needed when creating legal entities (paras. 8 – 10).

668. ***Ongoing due diligence***: There is no general requirement for lawyers to conduct on-going due diligence of the customer or ensure that documents, data, or information collected under the CDD process is kept up-to-date. Nonetheless, the Rules require that a lawyer must obtain "satisfactory evidence" on the nature and purpose of the business relationship between the client and any other party to the matter party when accepting instructions "at any time thereafter". The PD further requires lawyers to obtain satisfactory evidence of client identity when accepting instructions and on an ongoing basis when instructed for the five types of matters reflected in Rule 11(F)(1) of the Rules. The PD also emphasises the importance of this requirement by highlighting that there can be changes to instructions and/or changes to the relationship between the client and third party that could give rise to real suspicions or risk that the law practice is being used to launder money or finance terrorism (PD (D)(1) and (4).

Risk

669. ***Enhanced CDD measures on high risk customers:*** The Practice Direction indicates that lawyers should carry out certain kinds of enhanced CDD (*e.g.* determine the client's source of wealth) when acting for certain high risk customers – PEPs or dubious clients (*e.g.* known or suspected criminals). However, enhanced due diligence measures are not required more generally in relation to higher risk customers (*e.g.* to non-resident customers, legal persons or arrangements such as trusts that are personal assets holding vehicles, or companies that have nominee shareholders or shares in bearer form).

670. ***Simplified CDD measures on low risk customers:*** The following types of clients are totally exempt from CDD requirements: a ministry or department of the Government, an organ of State or a statutory board or a public company listed on the local securities exchange or one recognised within the meaning of the Securities and Futures Act (Rule 11D(3)-(4); Practice Direction, (C)(I)(4). This does not comply with the FATF Recommendations which only allow for simplified CDD measures to be applied to customers deemed to be low risk.

Timing of verification

671. Lawyers are required to verify the identity of a client before a starting work on any matter, including before a solicitor-client relationship is established. If a law practice is instructed on an urgent basis, verification of the client's identity is to take place "as soon as reasonably practicable" (Rule 11D; Practice Direction, (C)(I)(1-3). However, there is no additional requirement to ensure that the ML risks are effectively managed in such cases.

Failure to satisfactorily complete CDD

672. There is no general requirement that, if the lawyer is unable to obtain the required CDD information, he/she should not be permitted to open the account/perform the transaction. However, Practice Direction, (C)(I)(5) indicates that if the law practice has a secretive client who is reluctant to provide evidence to verify his/her identity, then the law practice must either refuse the retainer or cease to act. Also, if a client refuses or is unable to provide the satisfactory evidence as to the nature and purpose of the business relationship with the client, and the business relationship between the client and another party to the matter the lawyer/law practice shall not act or continue to act for the client (Rule 11F(3), or if further enquiry is required and the client's responses are not credible or the

lawyer's suspicions are not adequately allayed by the responses, the lawyer should not accept further instructions (PD(J). Additionally, there is no requirement to consider making an STR if CDD cannot be satisfactorily completed, as is required by the FATF Recommendations.

Existing customers

673. Subject to a review of the risk profile of the clients, for existing clients who have not been in contact with the law practice for five years or more, a full KYC check is required. For existing clients who have been in contact with the law practice for the last five years and who provided formal identification on first contact, full KYC details on the opening of a new matter should be obtained if the lawyer/ law practice is not satisfied that that the original identification documents were adequate (Practice Direction, (C)(IV)(1).

Effectiveness

674. Effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendations 6, 8-11 (DNFBPs other than lawyers)

675. Currently, other than for lawyers and trust companies that are regulated as financial institutions (see Section 3 of this report), there are no enforceable obligations for DNFBPs in relation to Recommendations 6 and 8-11, with the exception of some record-keeping requirements for auditors. However, auditing activity is not covered under the FATF Recommendations.

Applying Recommendation 6 (Lawyers)

676. Lawyers are required to implement procedures and systems to determine if a client is a PEP or the legal person/body is effectively controlled by a PEP (Practice Direction, (C)(V)(6). When a client is identified as a PEP, the following measures must be taken:

(a) The lawyer should obtain senior management approval to act for such a client (or when client is subsequently found to be such a person).

(b) He/she must take reasonable steps to establish the source of wealth/ funds of this client at the time of the instruction. The lawyer should also take reasonable measures to establish the source or funds/wealth if he/she is acting for a legal person and discovers that a controlling person is a PEP. Furthermore, Practice Direction (H)(1-5) prohibits a lawyer from accepting payments in cash of more than SGD 100 000 into his/her client account for any one transaction without first determining the source of funds of the client.

(c) The lawyer should also check, when instructed and on an ongoing basis, the nature and purpose of the business relationship that the lawyer is being instructed to act for on behalf of the PEP (Practice Direction (C)(V)(1-6).

677. While generally broad, the Practice Direction does not require lawyers to conduct enhanced ongoing monitoring on relationships with clients who are PEPs. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendation 8 (Lawyers)

678. Lawyers are required to pay attention to any ML threats that may arise from new/developing technologies which favour anonymity and should take measures to implement policies and procedures to prevent their use in ML schemes. These systems, procedures and controls should also be reviewed from time to time (Practice Direction, (F)(1-2).

679. Generally, lawyers are supposed to obtain customer identification information during a face-to-face meeting with the client. However, if the client is unable to meet the lawyer face-to-face (*e.g.* in the case of someone who is not resident in Singapore), the lawyer must ask for a certified true copy of the identity document that must provide the client identification information listed above in relation to Recommendation 5. Faxed or photocopied documents are not acceptable (Practice Direction, C(III)(1). Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendation 9 (Lawyers)

680. Lawyers are allowed to use intermediaries/third parties, such as search companies or credit reference agencies, to establish a client's identity. In such cases, they are required to obtain for the record the copies of documentation used for the identification and verification by the third party without delay. The lawyer must also be satisfied that the intermediaries/third parties being relied upon are reputable, that they will meet the KYC requirements set by the Rules and Practice Direction and that they are reliable (Practice Direction, (C)(I)(8-9) However, there is no requirement to ensure that the intermediary/third party is regulated and supervised in accordance with the FATF Recommendations, and has measures in place to comply with Recommendations 5 and 10. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

681. As well, determining whether the intermediary/third party is reputable and reliable, there is no requirement to consider whether the intermediary/third party is located in a country that does not adequately apply the FATF Recommendations). Furthermore, there is no provision that explicitly states that the ultimate responsibility for customer identification and verification remains with the lawyer who is relying on the intermediary/third party. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendation 10 (Lawyers)

682. Lawyers are required to retain client identification documents for not less than 5 years after the end of a matter. This rule applies to documents that were used to ascertain the nature and purpose of the business relationships and records of transactions undertaken on behalf of the client. It does not, however, generally apply to business correspondence. There is also no requirement to ensure that records are kept in such a manner as to permit the reconstruction of individual transaction.

683. For those records that are kept, lawyers are required to ensure that the documents and records retained are sufficient to enable information on the identity of the client and details of the relevant matter to be given to the Council of the Law Society, a police officer or a person appointed by the Council of the Law Society, subject to the obligations relating to professional communications (Rule 11H; Practice Direction, (G)(1 – 2)). It is not expressly stated that this information should be made available on a timely basis. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendation 11 (Lawyers)

684. The Practice Direction requires lawyers to consider suspect transactions that have no apparent commercial justification in relation to the complexity of the matter, quantum involved, any apparent economic or lawful purpose, and the business and risk profile of the client (Practice Direction I-1.). Lawyers are required to examine the background and purpose of transactions that are complex, unusual, large or have unusual patterns. These findings must be set out in writing (Practice Direction I 2). Such findings must be available in the event of an inspection by the council to evidence compliance with the Practice Direction. There is, however, no specific indication as to how long such findings must be kept. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

4.1.2 Recommendations and Comments

685. The Singapore authorities should adopt and implement comprehensive measures as contemplated in Recommendation 12 for real estate agents, dealers in precious metals and dealers in precious stones, accountants, and trust and company service providers (other than trust companies which are regulated as financial institutions). As casinos come into operation, Singapore authorities should ensure that adequate AML/CFT requirements are applied to that sector as well.

Lawyers

686. Lawyers are now subject to broader CDD requirements through the new Rules, and a new Practice Direction provides more detailed CDD requirements, including on the areas contemplated in Recommendations 6, and 8-11.

687. In relation to Recommendation 5, Singapore should ensure that all of the basic obligations are contained in law and regulation. As well, Singapore should enhance the CDD obligations by implementing requirements to:

(a) Conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data.

(b) Identify the beneficial owner of all customers (not just for corporate customers).

(c) Understand the ownership and control structure of the customer.

(d) Understand the nature and purpose of the business relationship in all cases required by the FATF Recommendations.

(e) Conduct ongoing due diligence on the customer, and ensure that CDD information is kept up-to-date.

(f) Broaden the categories of high risk customers to whom enhanced CDD measures must be applied.

(g) Ensure that, at least, simplified CDD is applied to the low risk customers identified in the Rules.

(h) Ensure that the ML risks are effectively managed when CDD cannot be completed at the start of the business relationship.

(i) Ensure that, in all cases, if the lawyer is unable to obtain the required CDD information, he/she is not permitted to open the account/perform the transaction.

(j) Consider making an STR if CDD cannot be satisfactorily completed.

688. In relation to Recommendation 6, Singapore should require lawyers to conduct enhanced ongoing monitoring on relationships with clients who are PEPs.

689. In relation to Recommendation 9, Singapore should implement a requirement to ensure that the intermediary/third party is regulated and supervised in accordance with the FATF Recommendations, and has measures in place to comply with Recommendations 5 and 10. As well, Singapore should implement a requirement to consider whether the intermediary/third party is located in a country that does not adequately apply the FATF Recommendations. A provision should also be enacted that explicitly states that the ultimate responsibility for customer identification and verification remains with the lawyer who is relying on the intermediary/third party.

690. In relation to Recommendation 10, Singapore should implement requirements to maintain business correspondence, ensure that records are kept in such a manner as to permit the reconstruction of individual transaction, and ensure that all records can be made available on a timely basis.

691. In relation to Recommendation 11, Singapore should implement a requirement that all findings relating to unusual transactions be kept for 5 years.

692. The authorities should ensure that the legal sector effectively implements the new requirements in relation to R.5, 6 and 8-11.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**NC**	• Real estate agents, dealers in precious metals and stones, accountants, and trust service providers (other than trust companies) and company service providers do not have any AML/CFT obligations pertaining to Recommendation 12. *Lawyers:* • The measures to implement Recommendation 5 suffer from the following deficiencies: - There is no specific requirement to conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data. - There is no specific requirement for lawyers to identify the beneficial owner for all customers or to determine if the customer is acting on behalf of another person. - There is no specific requirement to understand the ownership and control structure of the customer. - The requirement to understand the nature and purpose of the business relationship does not apply to all circumstances required by the FATF Recommendations. - There is no general requirement for lawyers to conduct on-going due diligence of the customer or ensure that information collected under the CDD process is kept up-to-date. - Enhanced due diligence is not generally applied to all high risk customers. - Certain specified categories of low risk customer are completely exempted from CDD requirements, rather than being made subject to simplified CDD measures. - There is no requirement to ensure that the ML risks are effectively managed when CDD cannot be completed at the start of the business relationship. - The prohibition on an account being opened or transaction performed if the required CDD information cannot be obtained is too narrow, and does not apply to all cases. - There is no requirement to consider making an STR if CDD cannot be satisfactorily completed. - Effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 6, there is no requirement to conduct enhanced ongoing monitoring on relationships with clients who are PEPs. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force. • The measures to implement Recommendation 9 suffer from the following deficiencies: - There is no requirement to ensure that the intermediary/third party is regulated and supervised in accordance with the FATF Recommendations, or has measures in place to comply with Recommendations 5 and 10. - There is no requirement to consider whether the intermediary/third party is located in a country that does not adequately apply the FATF Recommendations. - There is no provision that explicitly states that the ultimate responsibility for customer identification and verification remains with the lawyer who is relying on the intermediary/third party. - Effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 10, there is no requirement to maintain business correspondence, ensure that records are kept in such a manner as to permit the reconstruction of individual transaction, and ensure that all records can be made

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
		available on a timely basis. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 11, there is no express requirement that all findings relating to unusual transactions be kept for 5 years. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force.

4.2 Monitoring Transactions and other Issues (R.16)

(Applying R.13 to 15 & 21)

4.2.1 Description and Analysis

Applying Recommendation 13

693. The reporting requirements that apply to financial institutions under the CDSA (s.39) and TSOFA (s.8 and 10) apply to all persons, and therefore to all DNFBPs. For a full description of these obligations, including their deficiencies, see Section 3.7 above. The same criminal sanctions also apply for failure to adhere to these obligations. (See Section 2.1 above.)

694. All STRs must be reported directly to the police FIU, the Suspicious Transaction Reporting Office (STRO), which belongs to the police. While some regulators might require the reporting entities to extend a copy of the STRs to them, this requirement is in addition to the mandatory obligation to file the STR with STRO. The purpose of requesting to receive copies of the STRs is to check and improve, if necessary, related aspects of the supervision.

Lawyers

695. Lawyers are subject to the statutory requirement to report suspicious transactions. The STR reporting obligation has been referenced in Rule 11G of the amendments to the Legal Profession Rules and explained in the Practice Direction. Hence, a lawyer who fails to make a STR will, in addition to the criminal penalties under the CDSA, also be liable to disciplinary proceedings under the Legal Profession Act.

696. Section 39 of the CDSA provides that it is not an offence for an advocate and solicitor or his clerks or employees or an interpreter to fail to disclose any information or other matter which are items subject to legal privilege. Items subject to legal privilege are:

(a) Communications between an advocate and solicitor and his client or any person representing his client made in connection with the giving of legal advice to the client.

(b) Communications between an advocate and solicitor and his client or any person representing his client or between such an advocate and solicitor 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.

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

  (i) In connection with the giving of legal advice. Or

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

  When they are in the possession of a person who is entitled to possession of them, but excluding, in any case, any communications or item held with the intention of furthering a criminal purpose.

Applying Recommendation 14

697. The safe harbour and tipping off provisions under the CDSA that apply to financial institutions are equally applicable to DNFBPs. (See section 3.7 above for the full details.) As indicated, there are concerns about the fact that current tipping off provisions do not cover when a transaction is being processed or an STR being reported.

Applying Recommendation 15

698. There are currently no enforceable obligations relating to Recommendation 15 in relation to any category of DNFBP, other than lawyers and trust companies that are regulated as financial institutions.

699. Lawyers are required to develop internal policies, procedures and controls (including adequate management controls set by the proprietors, partners or directors of the practice) in order to satisfy the requirement of having "reasonable measures" to establish client identity and assess the risks of ML/TF faced by their law practice. These procedures and controls are to be audited by the Law Society to ensure that they are complied with (Practice Direction, (E)(1). However, the obligation does not extend to internal controls in relation to record retention, the detection of unusual and suspicious transactions or the reporting obligation. As well, there is no requirement in the Practice Direction to maintain an adequately resourced and independent internal audit function, appoint a compliance officer or establish screening procedures to ensure high standards when hiring employees. AML training is a requirement, but not CFT training. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

Applying Recommendation 21

700. There are currently no enforceable obligations relating to Recommendation 21 in relation to any category of DNFBP, other than lawyers and trust companies that are regulated as financial institutions).

701. Lawyers are required to develop internal policies, procedures and controls to ensure that they carry out enhanced due diligence on clients who are from a country that does not apply (or only partially applies) the FATF Recommendations (Practice Direction E-2). When deal with such clients, lawyers are required to document the background and purpose of any transactions that have no apparent economic or visible lawful purpose, and should maintain the written findings and have them available for the Council in the event of an inspection (Practice Direction I). As these measures were only recently enacted, it is not possible to assess their effectiveness.

Additional elements

702. The reporting requirement as provided for under Section 39 of the CDSA applies to all persons (not just financial institutions and DNFBPs) and, therefore, includes auditors.

Statistics and effectiveness

703. The following chart sets out a breakdown of the STRs received from the DNFBP sectors.

Breakdown of Suspicious Transaction Reports Received

	2004	2005	2006	2007 (as at 14 Nov.)
Accountants and Auditors	1	-	2	2
Lawyers and Notaries Public	-	-	2	2
Trust and Company Service Providers	3	1	1	8
Precious Stones and Metals Dealers	-	-	-	-
Real Estate Industry	6	-	-	14

704. The STR reporting obligation and the related obligations under the CDSA and TSOFA apply to every person. The supervisory authorities, in cooperation with STRO and CAD, and STRO and CAD also independently have made considerable efforts to raise awareness of this fact and educate the sectors concerned accordingly. However, the effectiveness of the reporting regime for DNFBPs has not been demonstrated, as the level of STRs from the DNFBP sectors remains very low, even though these requirements have been in place for over four years.

4.2.2 Recommendations and Comments

705. Meetings with the some members of the private sector (*e.g.* lawyers) have shown a general awareness of the STR reporting obligations. However, a large number of DNFBPs whom the assessment team met did not understand the reporting obligation. For instance, in a number of sectors, a generalised weakness in distinguishing situations in which an STR should be filed is evident. The reaction of "if such a situation arises we call CAD" seems to be quite widespread. On the one hand, this could lead to defensive reporting. On the other hand, STRO's independence from CAD seems not to be perceived by the large public, which could have negative effects on STRO. Singapore should conduct more outreach to DNFBPs to enhance compliance with the reporting obligation.

706. The fact that in many areas AML/CFT preventive measures are still missing contributes to the above-mentioned deficiency. Relevant measures should be issued to the various sectors still lacking them. Once introduced, intensive training efforts should be made.

707. Singapore authorities should rectify the deficiencies relating to its tipping off provisions.

708. Singapore should adopt more comprehensive requirements for R.15 and R.21 for all DNFBPs. The Practice Direction of the Legal Profession should extend the obligation of staff training to TF. Also, provisions for screening procedures for employees should be introduced.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**	• The measures to implement Recommendation 13 suffer from the following deficiencies: - The reporting obligation is not implemented effectively (lack of understanding about the reporting obligation, and low numbers of reports being filed even though the requirements have been in place for four years). - The limitations identified under Recommendation 13 with respect to the reporting obligation also affect compliance with Recommendation 16. • The limitations identified under Recommendation 14 with respect to the tipping off provision also affect compliance with Recommendation 16. • None of the DNFBP sectors (other than lawyers and part of the TCSPs, namely the trust companies) are subject to requirements relating to R.15 and 21. *Lawyers* • The measures to implement Recommendation 15 suffer from the following deficiencies: - There is no requirement to implement internal controls in relation to record retention, the detection of unusual and suspicious transactions or the reporting obligation. - There is no requirement to maintain an adequately resourced and independent audit function, appoint a compliance officer or establish screening procedures to ensure high standards when hiring employees. - There is no requirement to provide training that covers FT. - Effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007). • In relation to Recommendation 21, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007).

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
		Trust Companies • The limitations identified under Recommendation 15 and 21 with respect to financial institutions also affect compliance with Recommendation 16.

4.3 Regulation, Supervision and Monitoring (R.24-25)

4.3.1 Description and Analysis

Recommendation 24 (Supervision of DNFBPs)

Casinos[91]

709. The Ministry of Home Affairs ("MHA") is in the process of establishing a statutory board called the Casino Regulatory Authority ("CRA") to provide regulatory oversight and supervision of the casinos. The CCA provides for the CRA to license casino operators in Singapore.

710. The CCA provides the legislative and regulatory framework to help ensure that criminal activities associated with casino operations will not take root in Singapore. Sections 10, 15, 46, 63 and 85 of the CCA empower the CRA to investigate and probe into the casino operators' background, accounts and business links.

711. As the casino operators and their key employees have to be licensed by the CRA, only suitable persons will be licensed to operate the casino or to work in positions of influence in the casino. Having obtained the licence, the licensee must remain suitable throughout the validity period of the licence. Where and when there are material changes to the licensee's situation that could affect his suitability, the licensee will be required to report these changes promptly to the CRA. Apart from the casino operators and their employees, the CRA will also scrutinise the suitability of shareholders and business associates. Shareholders taking a 5%, 12% or 20% stake in the casino operator are required under sections 64 to 71 of the CCA to seek approval from the MHA. The casino operator is required to seek approval from the CRA for 'controlled' contracts, which are either contracts of significant monetary value or provide critical services to the casino, such as security and surveillance. Details of the controlled contract regime will be prescribed in the subsidiary legislation to be enacted under the CCA.

Lawyers

712. The competent authority for lawyers is the Law Society of Singapore. The Society is managed by the Council of the Society which consists of 15 elected members, as well as up to three members nominated to serve by the MinLaw, up to three members nominated by the Council as well as the immediate past President of the Council. It is staffed by a Secretariat, headed by a CEO, and has sufficient resources to perform its functions.

713. The Rules are issued under the Legal Profession Act and have the force of law. Breaches of the Rules may lead to disciplinary proceedings with penalties ranging from being struck off the roll, suspended from practice, a fine or a censure. Practice Directions issued under the Legal Profession Act are similarly enforceable if the breach amounts to misconduct.

714. The Law Society has adequate inspection and supervisory powers to perform its functions. To ascertain whether the AML/CFT requirements in the Rules or Practice Direction are being complied with, the Council of the Law Society may require a lawyer to produce documents or provide any

[91] It is planned that casino operators will have to implement a AML/CFT programme which shall include KYC and CDD measures, mandatory reporting for cash transactions above SGD 10 000 (approximately EUR 5 000), record keeping for transactions above SGD 5 000 (approximately EUR 2 500), mandatory reporting of suspicious transactions, and ongoing AML/CFT training for the employees. These measures are to be prescribed in AML regulations that are planned to be enacted pursuant to Section 200(2) of the CCA.

information or explanation. The documents, information or explanations obtained may be used as a basis for disciplinary proceedings under the Legal Profession Act.

Accountants

715. The Institute of Certified Public Accountants of Singapore (ICPAS) issues guidance to its members, including guidance on AML/CFT – the Revised Statement of Auditing Practice (SAP 19) (dated 7 April 2005) on Guidance to Auditors on Money Laundering and Terrorist Financing and auditing standards in relation to the consideration of laws and regulations and fraud in an audit. Compliance with the prescribed standards, including SAPs is monitored under a Practice Monitoring Programme (PMP) that is carried out by practice reviewers who are appointed by ACRA.

716. Where a public accountant fails the practice review, the Public Accountants Oversight Committee may: impose conditions on the public accountant's ability to provide accountancy services; require the public accountant to undergo and satisfactorily complete a remedial programme or take other steps to improve his/her practice; give an undertaking; or refuse to renew, suspend or cancel the public accountant's registration (s.38 Accountants Act). However, the PMP does not apply when auditors are performing other types of accounting services, i.e. non-auditing work (*e.g.* giving advice or administrative services in the ordering of personal affairs; advising on the setting up of trusts, companies or other bodies; arranging loans; acting as a trustee, nominee or company director). Accordingly, no authority or SRO has been designated responsible for ensuring that public accountants or other accountants providing such services comply with their AML/CFT obligations (which currently only extend to the reporting obligation).

Dealers in precious metals and stones

717. No authority or SRO has been designated responsible for ensuring that dealers in precious metals and stones comply with their AML/CFT obligations (which currently only extend to the reporting obligation). The majority of dealers are members of the Singapore Jewellers Association.

Real estate agents

718. Estate agencies in Singapore are licensed by the Inland Revenue Authority of Singapore (Comptroller of Property Tax) (IRAS) under the authority of the Appraisers and Housing Agents Act. Only estate agencies are licensed, not individual agents. No authority or SRO has been designated responsible for ensuring that real estate agents comply with their AML/CFT obligations (which currently only extend to the reporting obligation).

Company service providers

719. Singapore regulates company service providers (although not for AML/CFT purposes). Only "prescribed persons" under the CA, LLPA and BRA may file documents on behalf of third parties. The list of prescribed persons includes lawyers, accountants registered with the Institute of Certified Public Accountants of Singapore, a member of the Singapore Association of the Institute of Chartered Secretaries and Administrators, a corporate secretarial agent, and members of other prescribed professional associations (s.12A CA; s.42 LLPA). Lawyers and accountants who act as company service providers (the largest group) are subject to supervision by their respective professional associations. Singapore is studying the possibility of a more detailed framework for such regulation. Company service providers who operate by using a business vehicle (such as a sole proprietorship or company) will also be subject to the same legal requirements imposed on those entities as other business entities are with respect to disclosure of information on formation.

720. Prescribed persons who apply are issued with a "professional number" by ACRA to be able to access *Bizfile* (the on-line corporate and business information system referred to earlier). Only prescribed persons with a professional number can access *Bizfile* on behalf of third parties. Hence,

ACRA is fully aware, and has a detailed register, of company service providers. However, ACRA does not monitor or supervise company service providers for AML/CFT purposes.

Trust service providers

721. Whoever carries on any trust business (as defined by the First Schedule of the Trust Companies Act) in or from within Singapore has to be licensed as a trust company except when the person is a specified person in accordance with the Second Schedule or is exempt from the licensing requirement (s.15(1) TCA and the Trust Companies (Exemption) Regulations 2005, such as lawyers and public accountants. Trust companies are defined as financial institution and regulated by MAS under the Trust Companies Act. They are subject to the full range of AML/CFT requirements imposed on the financial industry (see section 3 of this report for a detailed description of these requirements).

722. For persons engaged in the activities set out in the Second Schedule of the Trust Companies Act no authority has been designated responsible for ensuring that they comply with their AML/CFT obligations (which currently only extend to the reporting obligation). For persons or classes of persons exempted from the licensing requirement when providing the type of trust services as described for each class in the Trust Companies (Exemption) Regulations 2005 other than lawyers, no authority has been designated responsible for ensuring that they comply with their AML/CFT obligations (which currently only extend to the reporting obligation).

Recommendation 25 (Guidance for the DNFBP sectors)

723. The following AML/CFT guidance has been issued to various DNFBPs:

S/No.	Description	Sector	Relevant Authority
1	Practice Direction of the Council on Prevention of Money Laundering and the Funding of Terrorist Activities	Lawyers / law practice	The Law Society of Singapore
2	FAQ on Law Society's Rules and Practice Direction on Anti-Money Laundering and the Prevention of Terrorist Financing	Lawyers / law practice	The Law Society of Singapore
3	Summary on the Practice Rules to Combat Money Laundering and Terrorist Financing (Law Gazette September 2007)	Lawyers / law practice	The Law Society of Singapore
4	Revised Statement of Auditing Practice (SAP) 19 on Guidance to Auditors on Money Laundering and Terrorism Financing (relevant only as far as STR and related obligations are concerned as it covers otherwise the professional conduct when auditing, not the activities covered by Rec. 12)	Accountants	Institute of Certified Public Accountants of Singapore
5	Guidelines on the Prevention of Money Laundering for Real Estate Agents	Real Estate	IRAS
6	Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism for Dealers in Precious Metals and Stones	Dealers in Precious Metals and Stones	Singapore Jewellers Association (private industry organisation)

724. CAD frequently conducts outreach to various sectors, including the DNFBP. During the outreach, CAD provides guidance on AML/CFT and the various relevant legislations. Apart from providing an overview of Singapore's AML / CFT legislation, and in particular, the requirement to report STRs, these sessions also provide insights into:

(a) The importance of reporting STR to enhance Singapore's AML / CFT regime.

(b) Common indicators of a suspicious transaction pertinent to the particular sector.

(c) Sanitised case studies and trends relevant to the industry.

(d) The necessity to conduct CDD and continuing CDD, including useful tips on how CDD could be conducted.

(e) The importance to maintain adequate records, particularly for the purposes of review.

(f) The requirement to ensure that the clients are not PEPs, etc.

725. STRO/CAD makes reference to the MAS Notices in its outreach programmes to the financial sector. STRO is developing its own internal set of guidelines, which will be used to educate the general public/ institutions in the enhancement of their AML/CFT measures and knowledge. CAD has published the 2nd edition of AML/CFT Handbook, which is available online at STRO / CAD website and accessible by members of the public, including DNFBPs.

Casinos

726. Section 200(2)(t) CCA provides that the CRA may, with the approval of the Minister make regulations for or with respect to AML requirements. The provision is silent on regulations for or with respect to CFT requirements. Such regulations could, however, be made under the general clause of subsection (2)(v) or under subsection (1) CCA.

Lawyers

727. The Council of the Law Society has amended the Legal Profession Rules with AML/CFT measures and supplemented and specified them in more details in a Practice Direction. The latter is rather complex and the Council has made available additional guidance in the form of an FAQ section on this topic on its website and a summary of the new Rules and the Practice Direction published in the Law Gazette of September 2007. The Practice Direction itself also includes STR Reporting Forms for natural and legal persons in its Annex C (Practice Direction, section (A)(9-12), Annexure C).

Real estate agents

728. IRAS has published a set of "Guidelines on Preventing ML for Real Estate Agents". The guidelines explain the concept of ML/FT and set out the applicable provisions of the CDSA and TSOFA on the criminalising of the ML/FT offence, the requirement to disclose suspicious transactions, the tipping-off offence and failure to cooperate with law enforcement agencies. The guidelines also provide examples of red flag indicators of ML/FT. However, these guidelines apply only to reporting obligations and do not cover most issues under the FATF Recommendations (*e.g.* CDD, record keeping, internal controls).

Dealers in previous metals and previous stones and trust and company service providers

729. The Singapore Jewellers Association (SJA) has published and sent to its members on 3 September 2007 a set of "Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism for Dealers in Precious Metals and Stones". The guidelines explain the concept of ML/FT and set out the applicable provisions of the CDSA and TSOFA on the criminalising of the ML/FT offence, the requirement to disclose suspicious transactions, the tipping-off offence and failure to cooperate with law enforcement agencies. The guidelines also provide examples of red flag indicators of ML/FT. However, these guidelines apply only to reporting obligations and do not cover most issues under the FATF Recommendations (*e.g.* CDD, record keeping, internal controls).

730. CAD works with the private sector (SJA) to conduct workshops to educate jewellers on the reporting of suspicious transactions. In particular, CAD and STRO have participated in two outreach seminars to raise awareness on the reporting and related CDSA and TSOFA requirements, although based on the meeting with the private sector, the assessment team found the level of awareness concerning the obligations of dealers in relation to filing STRs to be low. The association is planning to revise their Trade Code of Ethics and Business Practices in the first quarter of 2008.

Trust and company service providers

731. AML/CFT guidelines for trust service providers (other than trust companies and lawyers and to some extent accountants) and company service providers have not been issued.

Accountants

732. ICPAS has issued Guidance to Auditors on Money Laundering and Terrorism Financing (SAP 19). SAP 19. focuses in general on professional duties of accounting firms and individual auditors in the context of their incidental work and not on the activities covered by Recommendation 12. Nonetheless, section 14 advises that the guidance should be applied similarly to services that the public accountants might provide outside of their incidental work, such as acting as a trustee or offer safe custody services, activities within the purview of Recommendations 12. It remains unclear whether this direction refers to the guidance on the reporting obligations or also to other guidance such as the clarifications on KYC and documentation requirements.

733. As the STR reporting and related obligations under the CDSA and TSOFA are obligations applicable to all persons, the extensive explanations on these obligations in the Guidance are of a general validity and suitable to educate members of the accounting profession beyond their professional duties. Particular mention in this respect should be made of Appendix B: Summary of Basic Criminal Offences Under Anti-Money Laundering Legislation, Appendix C: Summary of Basic Criminal Offences under Terrorism-Financing Legislation, Appendix F: Indicative Report Content. Further explanations are contained in Paragraphs 9, 23, 24, 28, 47 and 48 and 49 of the Guidance. Paragraph 48 comprises the duty to consider if a STR needs to be filed when an auditor while performing his incidental work, comes across a situation that raises a suspicion that ML or TF has occurred. This could lead to an auditor being liable for contravening provisions on professional conduct in addition to being criminally liable for it.

734. Another educative tool of this Guidance is Appendix E: Factors indicating an increased Risk of Money Laundering, containing a list of common indicators and a list of industry-specific indicators which covers the following industries: Financial Entities, Moneylenders, Life Insurance Companies, Brokers and Agents, Securities Dealers, Foreign Exchange Dealers and Money Services Businesses, Accountants, Real Estate Brokers and Sales Representatives, Casinos and other Gaming/Betting Organisations, and Factors arising from action by the entity or its directors.

735. The Guidance's requirements on AML/CFT training for this sector may also be seen to have an awareness raising effect beyond the professional duties of an auditor. (Para 75 – 79, SAP 19).

Statistics and effectiveness

736. The CCA establishes a legislative framework for supervising casinos for compliance with AML/CFT measures. However, the designated authority (the CRA) has not yet been established, and casinos do not yet exist in Singapore. Consequently, these measures have yet to be implemented.

737. Lawyers are supervised for compliance for AML/CFT requirements; however, as the regime is very new, its effectiveness cannot yet be assessed. Real estate agents and dealers in precious metals and stones and TCSPs (other than trust companies that are regulated as financial institutions as described in

section 3 of this report) have not been issued with AML/CFT measures (other than the reporting obligations) and are therefore not monitored for it.

738. Although accountants have been issued some AML/CFT guidance, it applies to their incidental work and does not cover the activities that should be covered in accordance with the FATF-Recommendations.

4.3.2 Recommendations and Comments

739. Singapore should implement comprehensive AML/CFT obligations for real estate agents, dealers in precious metals and stones, accountants, and trust and company service providers (other than trust companies which are regulated as financial institutions), and ensure that these sectors are subject to an effective AML/CFT oversight mechanism. Additionally, a more comprehensive mechanism to monitor lawyers for a broader range of AML/CFT measures should be implemented. When developing its casino sector, Singapore should ensure that the regulations issued are comprehensive and subject to adequate supervision as well.

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBPs)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**NC**	• No AML/CFT supervisory regime for real estate agents. • No AML/CFT supervisory regime for dealers in precious metals and stones. • No AML/CFT supervisory regime for accountants. • No AML/CFT supervisory regime for trust and company service providers (other than trust companies). • No comprehensive AML/CFT monitoring for lawyers, and the effectiveness of the existing regime cannot yet be assessed.
R.25	**LC**	• No issued guidance for trust service providers (other than trust companies and lawyers) or company service providers. • Existing guidelines for real estate agents, accountants, and dealers in precious metals and stones are not comprehensive. • No general or specific feedback given to DNFBPs concerning the reporting obligation.

4.4 Other Non-Financial Businesses and Professions/Modern Secure Transaction Techniques (R.20)

4.4.1 Description and Analysis

740. The reporting requirements that apply to financial institutions under the CDSA (s.39) and TSOFA (s.8 and 10) apply equally to all non-financial businesses and professions. For a full description of these obligations see section 3.7 of this report.

741. In addition, CAD actively identifies businesses, for example online payment systems, that pose a ML/TF risk and conducts outreach to create awareness about STR reporting. CAD has also engaged Singapore Turf Club and Singapore Pools on this issue. The two operators have incorporated STR requirements into their workflow. The Turf Club provides horse racing and totalisator services while Singapore Pools runs lottery services and football betting operations island-wide. Both gambling operators are owned by the Singapore Totalisator Board, a statutory board under the Ministry of Finance.

742. MAS is empowered under the Payment System (Oversight) Act 2006 to supervise payment system operators and participants. MAS' role in the oversight of payment and settlement systems is to promote the safety and efficiency of these infrastructures.

743. On a broader level, the Singapore Government has actively promoted cashless transactions to increase efficiency. The amount of currency in circulation (SGD 17.6 billion in 2006) as a percent of GDP has declined significantly from 11.6% in 1990 to 8.4% in 2006, which is low compared to other countries. In particular, Singapore has been developing more advanced and secured payment systems over the past few years. Transaction volume for the secured automated systems has been increasing steadily, which is further evidence of a reduction in Singapore's reliance on cash transactions. Examples of non-cash payment systems that have been implemented include:

(a) **Cheques:** The cheque clearing systems are designated payment systems regulated under the Payment Systems (Oversight) Act. In 2006, the Automated Clearing house processed 83 million SGD-denominated cheques and 881 000 USD-denominated cheques, with total values of SGD 468 billion and USD 29 billion respectively.

(b) **Interbank GIRO (IBG)**: This allows customers of a participating bank to transfer funds through direct debits and credits, to accounts in another participating bank. Interbank GIRO Clearing Services are conducted through a designated Automated Clearing House. The number of transactions processed has been showing a year on year growth of approximately 7% since 2004, to reach 78 million in 2006. The value of IBG transactions processed in 2006 was SGD 152 billion, 14% higher than 2005. The IBG system is a designated payment system under the Payment Systems (Oversight) Act.

(c) Credit/Charge Cards – The statistics of credit/charge card usage have been on the rise:

Year	Number of cards (Main)	Number of cards (Supplementary)	Total card billings in millions
2004	2985973	946784	14046.5
2005	3415507	1026516	16073.2
2006	3968044	1121932	18639.9

(d) **Debit cards (PIN-based debit cards and signature-based debit cards):** Debit cards allow cardholders to make payments and cash withdrawals from their deposit accounts through an Automatic Teller Machine (ATM) or Electronic Funds Transfers at Points of Sale Terminals (EFTPOS). As at 31 December 2006, there were about 70 000 EFTPOS terminals in Singapore. 154 million debit card transactions worth SGD 14.6 billion passed through the EFTPOS and ATM system in2006, indicating a growth of 11% in number of transactions and 26% increase in total value.

Year	Number of transactions (million)	Growth (Year on year) (%)	Value of transactions (billion)	Growth (Year on year) (%)
2004	121	N.A	9	N.A
2005	139	15	11.6	29
2006	154	11	14.6	26

744. One area of concern for the assessment team is the fact that Singapore issues banknotes of SGD 10 000 (approximately EUR 5 000). (A recommendation was made in the last mutual evaluation of Singapore to consider discontinuing this practice.) There are no requirements for banks or other professions when dealing with these notes. Singapore authorities note that the CDD requirements for unusual transactions will apply and financial institutions and merchants would be generally cautious about accepting high denomination notes.

745. However, in common practice, to guard against money laundering, fraud and counterfeit notes, banks check the serial number of high denomination notes presented against a list of loss/stolen notes, which is circulated by the Association of Banks. In addition, the banks record the identity of person presenting the SGD 10 000 note, serial number of the note and the account into which the note is paid into. The banks will also record the identity of the person drawing SGD 10 000 notes and the

serial number of these notes. Some banks do not accept SGD 10 000 notes from non-account holders or restrict notes exchange to no more than SGD 20 000. Some retailers for high value goods adopt the same practice of recording the details of customers using high denomination notes.

4.4.2 Recommendations and Comments

746. Singapore has extended AML/CFT reporting obligations to all persons, which thus includes all other businesses and professions in Singapore. Singapore has also taken some measures to encourage the development and use of modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering. However, the issuing of SGD 10 000 banknotes is still of some concern; Singapore authorities should consider whether it should continue issuing these notes and/or develop requirements for when dealing with them.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**LC**	• The issuing of the SGD 10 000 note is of some concern.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to Beneficial Ownership and Control Information (R.33)

5.1.1 Description and Analysis

Central Registration System

747. ACRA is the central registration authority in Singapore for business entities. ACRA maintains a Register containing information on entities, including ownership and control of companies and limited liability partnerships. Supplementing this information is a requirement for entities to maintain information on their premises (such as shareholder registers) which may be, in some instances, available for public inspection.

748. In order to incorporate a company an applicant must submit Articles and a Memorandum to ACRA in addition to other prescribed documents. Company Articles stipulate rules governing internal management. The information in a Memorandum includes:

- Name of the company.
- Location of the registered office;
- Liability of the members;
- Company's capital structure.
- Names of the members (shareholders) and the number of shares subscribed by them.
- Principle activities of the company (optional).

749. ACRA provides an electronic filing system called "*Bizfile*" which permits individuals to file incorporation and other documents on-line without visiting the ACRA offices. In order to access *Bizfile* an applicant must have a "*Singpass*" ("Singapore Personal Access") which is a personal access code permitting entry to many government services through an on-line system. Only Singapore citizens, permanent residents, employment pass and dependent pass holders can have a *Singpass*. Personal identification information is required and verified prior to issuance of this access code.

750. ACRA is not required to verify the accuracy of any information provided in the incorporation documents. Thus, there is no guarantee that the information is reliable, but filing of false information is an offence punishable with imprisonment (s401 CA; s45 LLPA). A company must have at least one shareholder who can either be an individual or a company (unless the company is an "exempt private company"[92]). Details of the shareholders must be filed and appear on ACRA's public file. On incorporation, a company must:

- Appoint a director (or directors).
- Appoint a company secretary.
- Establish various company registers including registers of members, substantial shareholders, debenture holders, directors, secretaries and auditors.

751. Company registers in addition to accounting records and official minute books must be available at the registered office address and be available for inspection by the company's members.[93] Under Singapore law, nominee directors are permitted.

752. Overall, ACRA is a good depository concerning legal ownership and control; however, it does not necessarily contain information concerning beneficial ownership and control, for the reasons specified below.

Companies

Register of Shareholders and Disclosure of Beneficial Ownership

753. The register of members must include the names and addresses of each member (shareholder), the date on which the entry is made, and details about the number and class of shares held by each shareholder. Failure to maintain the register is an offence (s190 CA). The register is open to public inspection (see s192 CA). Singapore law permits nominee (trustee) shareholders.

754. ***Private companies***: Where the shares are held in trust for a third party beneficial owner, the trustee may request that the shares be marked in the respective registers to identify them as such – but this is only at the request of the trustee (s 195(3) CA). The company is not obliged to seek or disclose the beneficial owner of shares to any person, including ACRA.

755. ***Public companies***: A publicly listed company is required to keep a register of substantial shareholders at the registered office and the register must be open for inspection by a member of the company without charge and by any other person on payment of a sum not exceeding SGD 2 for each inspection (s 88(2) CA). A substantial shareholder includes both the direct and beneficial owner who holds not less than 5% of the total votes attached to all the voting shares of the same class, in the company. To ensure that the register of substantial shareholders is kept up to date:

- Any person who becomes or ceases to be a substantial shareholder, or whose substantial interests changes, must report that fact to the company within two days (ss.82 and 83 CA).
- Publicly listed companies are empowered to request members to disclose if they hold shares as beneficial owner or as a trustee and must include that information in the company register (s.92 CA).

---

92 An "exempt private company" is one which has not more than 20 shareholders who are all natural persons or one that is wholly owned by the Government (by notification in the Gazette). Exempt private companies are not required to appoint auditors.

93 Other non-statutory books include the register of transfer of shares, register of application and allotment of shares, register of documents sealed, and finally the register of important documents.

756. These disclosure requirements do not apply to shareholders holding less than 5% of the total voting shares.

Changes in Shareholders

757. ***Private companies***: On incorporation, share allotment information (details of subscribers and shares issued) must be reported to ACRA. When ownership changes occur (other than a return of allotment) companies may report those changes immediately or at the annual reporting in an Annual Return. If reported immediately, companies must include notification of every other transfer effected prior to the date of the relevant notice. On the other hand, if reported at the annual reporting, only the current owner is required to be reported. There is no obligation to report previous transfers within the year. When there are more than 50 shareholders, only the top 50 shareholders who hold the most number of shares after the transfer need to be reported to ACRA (s.128A).

758. ***Public companies***: Companies publicly listed on a stock exchange in Singapore, need not furnish the particulars of their shareholders because public companies are subject to regulatory disclosure requirements. Much of the information relating to public companies is made available publicly and/ or independently checked by exchanges and external auditors. When shares are issued for non-cash consideration, sufficient justification and evidence of the consideration shall be reported to ACRA.

Limited Liability Partnerships

759. Two or more persons (including a body corporate – s 7 LLPA) who enter into a partnership to carry out business as a limited liability partnership are required to register their partnership under the LLPA. ACRA requires the following information to establish a LLP:

- Name and general business of the LLP.
- Registered office in Singapore.
- Name, identification, nationality and place of residence of every partner. Where a partner is a body corporate, the corporate name, place of incorporation or registration, registration number and registered office of the body corporate to which all notices and communications may be addressed is required.
- Name, identification, nationality and place of residence of every manager and, where a manager is a body corporate, the corporate name, place of incorporation or registration, registration number and registered office of the body corporate to which all notices and communications may be addressed.

760. The following LLP information must be reported annually to ACRA:

- Particulars of the persons who formed the limited liability partnership.
- Name of at least one local manager who is a natural person of full age and capacity.
- Changes to registered information.
- Declaration of solvency or insolvency (confirming if the LLP is able to pay its debts as they become due in the normal course of business).

761. This information is publicly available. But, the LLPA does not require collection of shareholder information on partners who are bodies corporate nor does the LLPA prohibit nominee partners in a limited partnership. This limits access to beneficial ownership for LLPs.

Foreign Companies

762. Foreign companies (defined under the Companies Act s 4[94]) include companies and limited liability partnerships incorporated outside Singapore but which "carry on business" (in accordance with the definition of that term in CA s.366) in Singapore.

763. Foreign companies are required to register a branch in Singapore before commencing business and, under section 368 of the CA, must file a number of pieces of information with ACRA including certified copies of the certificate of incorporation, memorandum and articles, and a list of directors containing similar particulars as for Singapore companies. After registration a foreign company is subject to similar domestic company reporting requirements including notification to ACRA of any changes in the directors of the foreign company. But foreign companies are not required to keep information on shareholders, nor changes to shareholdings, at their registered Singapore office unless one or more of the shareholders are Singapore residents. Information in relation to the resident shareholders and any changes thereto of foreign companies must be kept at the registered office or in a branch register (s.379 CA).

Company Service Providers

764. Singapore regulates company service providers. See section 4.3 of this report for an overview.

Access to Information by Competent Authorities

765. Competent authorities, including law enforcement, regulatory and supervisory authorities have a wide range of powers to obtain access to business information from companies and LLPs as follows:

Access powers of law enforcement authorities

766. The Singapore Police (including Suspicious Transaction Reporting Officers) have a variety of enforcement powers which may be used to secure business information including:

- Power to question persons/witnesses (including bodies corporate - Interpretation Act) acquainted with the facts and circumstances of a case (s.120 and 121 CPC). This power may be used to ask questions of a company into the beneficial ownership of shares.
- Production power (s.58 CPC and s.30 CDSA) to compel production of any document or thing, including financial information, for the purposes of any investigation, inquiry, trial or other proceeding.
- General seizure power (s.68 CPC) to seize property under circumstances which create a suspicion of the commission of any offence (including money laundering).
- Search warrants issued by a court (s.61 CPC and s.34 CDSA).

Access powers of regulatory and supervisory authorities

767. ***Companies***: Under Part II of the CA there are a variety of powers to compel corporations to disclose information to the regulatory or supervisory authorities. For instance, under section 8A, the responsible Minister or his designate may compel a company to produce (and make copies of) any books relating to the affairs of the company. This power includes the power to question corporate

[94] Companies Act s 4: "foreign company" means —
(a) A company, corporation, society, association or other body incorporated outside Singapore; or
(b) An unincorporated society, association or other body which under the law of its place of origin may sue or be sued, or hold property in the name of the secretary or other officer of the body or association duly appointed for that purpose and which does not have its head office or principal place of business in Singapore.

authorities on any matter relating to the documents. It is an offence to refuse to produce or any answer questions. In addition a magistrate may issue a search warrant under section 8B to seize those books that have not been produced when required under section 8A. In addition, under Part IX of the CA, the Minister responsible for ACRA also has powers to conduct inquiries through inspectors into the business affairs of a company (including a foreign company) where it is in the public interest to do so or where offences are suspected. Inspectors under this power may seize all books and documents of the company and question any officer or agent of the company.

768. ***Limited Liability Partnerships***: Likewise for limited partnerships, under section 43 of the LLPA, the Registrar of LLPs (the supervisory authority under the LLPA) or his designated inspector has the power at all reasonable times to enter into any LLP premises and make examinations or inquiries as may be necessary for the purposes of administering the Act including the right to compel disclosure of books. The Registrar also has a general power of questioning (which answers shall be in writing or orally) – it is an offence to refuse to cooperate. ACRA also has general investigation and enforcement powers to question and to call for information in any case where an offence under the Acts administered by ACRA is suspected (s31 Accounting and Corporate Regulatory Authority Act).

Access in a timely fashion to adequate, accurate, and current beneficial ownership and control information

769. Information filed with ACRA in relation to companies and LLPs is publicly available for a small fee and available to law enforcement and other competent authorities.

770. Where beneficial ownership and control details are lacking on the public register there are mechanisms to secure some information should competent authorities require it. This is constrained to some degree by the fact that neither the CA nor the LLPA require beneficial ownership and control information to be collected and kept with companies or LLPs. This is problematic for companies given the right to hold shares in trust and for LLPs, given that the LLPA does not require information to be collected for bodies corporate who are limited partners. Thus, a mutual legal assistance procedure would have to be used to obtain any information on foreign beneficial ownership, which would not provide timely access to beneficial ownership information.

771. Apart from the information contained in the ACRA's registry and the records maintained by companies and LLPs, which contains limited information on shareholders and partners, there is no other mechanism to ascertain beneficial ownership information for business entities in Singapore except through powers exercised by law enforcement and regulatory authorities.

Bearer shares

772. Bearer shares in Singapore are not permitted. Companies incorporated in Singapore are required to issue registered shares only. Moreover, section 66 of the CA prohibits a company from issuing share warrants permitting the bearer to acquire specified shares and which enables the shares to be transferred by delivery of the warrant.

5.1.2 Recommendations and Comments

773. ACRA operates a central system of registration for all business entities in Singapore including foreign companies. ACRA also operates a sophisticated electronic filing and access to corporate information system with safeguards (such as *Singpass*) in place to ensure that those with access to *Bizfile* (including company service providers) are properly identified and regulated. Although company service providers are supervised by ACRA, anyone with a Singpass can incorporate a company. There is no requirement for beneficial ownership to be collected either by the company (other than publicly listed companies), or by ACRA. Consequently, even though law enforcement powers are sufficient to obtain such information where it is available, that does not assist them if such information does not exist. Likewise, although the supervisory authorities may compel a company to

produce its books, that does not assist if the books are not required to retain beneficial ownership information (e.g. in the case of private companies which are not required to seek the beneficial owner of shares, or in the case of an LLP which is not required to collect shareholder information on partners who are legal persons).

774. Singapore should broaden the requirements on beneficial ownership so that information on ownership/control is readily available in a timely manner. This could include, for example, restricting the use of nominee directors and shareholders or alternatively requiring full disclosure and reporting of third parties; or obliging legal persons to record full information on beneficial ownership and control in its register which would be available to law enforcement and regulatory/supervisory authorities.

5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	**PC**	• While the investigative powers are generally sound and widely used, there are limited measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Information on the company registrar pertains only to legal ownership/control (as opposed to beneficial ownership), is not verified and is not necessarily reliable. • Foreign companies are not required to keep information on shareholders, nor changes to shareholdings, at their registered Singapore office unless one or more of the shareholders are Singapore residents. • Limited liability partnerships are not required to collect shareholder information on partners who are bodies corporate.

5.2 Legal Arrangements – Access to Beneficial Ownership and Control Information (R.34)

5.2.1 Description and Analysis

775. Trusts are not separate legal entities in Singapore, and unlike company law there is no central or other registry for the registration of trusts. Registration is required if the trust has a business name or if the trust/trustee requires a licence for business activities. And if the trustee is a corporate entity (such as a Trust Company), it must comply with the registration and reporting requirements for a company with ACRA.

776. Most complex trust arrangements in Singapore are established by using a Trust Company or a lawyer. Trust Companies are defined as financial institutions and regulated by MAS under the Trust Companies Act. A Trust Company that acts as a trustee of an express trust is required to keep books (under s 28(1), Trust Companies Act) which must contain, among other things:

- Particulars (including the name and address) of every settlor of a trust.
- To the extent known, every beneficiary of the trust, (Part V, Trust Companies Regulations) including particulars that satisfy such notices as may be issued by MAS – which includes AML/CFT requirements in MAS Notice TCA-NO3, 29 December 2006.

777. As to the last point, MAS Notice TCA-NO3 (section 4.3) requires that a Trust Company shall identify each trust-relevant party with whom the trust company comes into business before the trust is constituted and with respect to a beneficiary as soon as practicable after the beneficiary becomes identifiable, and, in any case, before making a distribution to that beneficiary. Hence, even if a beneficial owner is not identified at the time of constituting the trust, the trust company must perform the full range of CDD in accordance with MAS rules on the beneficiary prior to disbursing any benefits to that person. In effect, this obligation could block the entitlement of a beneficiary to take a benefit under a trust until full identification of that person is made.

778. Nevertheless, while competent authorities have powers to access information on beneficial ownership in trusts, availability of that information is limited by the fact that only trusts administered by trustee companies and trust company service providers are obliged to maintain such information.

779. Law enforcement agencies have powers to obtain information on the owners of trusts under criminal investigation. These powers include powers to compel production of financial records, trace property ownership, search premises for evidential material and summons a person to give evidence under oath. Some of these powers would not be productive of beneficial control information of any specific trust, since only trusts administered by trustees companies and TCSPs are obliged to maintain that information (see preceding paragraph). Other methods may produce this information (*e.g.* statements) but in those cases law enforcement can only produce this information in the context of a criminal investigation.

780. In addition, where the trustee is a Trust Company incorporated under the Companies Act, the full range of administrative powers of access (discussed in section 5.1 of this report) apply.

5.2.2 Recommendations and Comments

781. Many trusts in Singapore are administered by Trust Companies which are financial institutions regulated by MAS (and specifically by AML/CFT rules under MAS Notices) and also subject to the regulatory oversight of ACRA with respect to company law obligations. While competent authorities have powers to access information on beneficial ownership in these trusts, trusts not administered by trustee companies are not obliged to maintain such information. Singapore should broaden the requirements on beneficial ownership so that information on ownership/control for all trusts (not just those administered by trust companies) is readily available in a timely manner.

5.2.3 Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
R.34	**PC**	• While competent authorities have powers to access information on beneficial ownership in trusts, availability of that information is limited by the fact that only trusts administered by trustee companies and trust company service providers are obliged to maintain such information.

5.3 Non-Profit Organisations (SR.VIII)

5.3.1 Description and Analysis

Characteristics of the Non-profit organisations (NP0) Sector

782. Singapore's NPO sector is significantly populated by two forms of entities:

1) ***Charities***: Entities established exclusively for charitable objects including relief of poverty, advancement of education, advancement of religion and other purposes beneficial to the community.

2) ***Institutions of a Public Character (IPCs)***: NPOs whose activities are beneficial to the community as a whole, and not confined to sectional interests or group of persons based on race, creed, belief or religion, unless otherwise approved by the Commissioner of Charities.[95] IPCs are authorised to

[95] Examples of IPCs include hospitals not operated or conducted for profit; public or benevolent institutions; universities or a public fund for the establishment, maintenance, enlargement or improvement of a university; a public fund established and maintained for the relief of distress among members of the public; and others.

receive tax-deductible donations i.e. donors are given tax deduction for donations made to these organisations. Most IPCs are charities; with others being sports associations.

783. According to the Commissioner of Charities 2005 Annual Report (the last report filed) the NPO sector was broken down as follows:

NUMBER OF REGISTERED CHARITIES				
Charitable Objective	**As at 31 Dec 2004**	**Registered in 2005**	**Deregistered in 2005**	**As at 31 Dec 2005**
Relief of Poverty	14	0	0	14 (1%)
Mixed Activities	193	12	1	204 (11%)
Advancement of Education	216	11	2	225 (12%)
Purposes Beneficial to the Community	392	25	5	412 (23%)
Advancement of Religion	932	28	8	952 (53%)
TOTAL	**1 747**	**76**	**16**	**1 807 (100%)**

Source: Singapore Government Charity Portal.

784. According to the Commissioner of Charities, as of the date of the on-site visit (September 2007) there were approximately 1,900 charities in Singapore, 900 of which are IPCs, broken down in roughly the same proportions.

Reviews of the Domestic Non-Profit Sector

785. Two comprehensive reviews (2004 and 2006) were undertaken by an inter-governmental group, referred to as the "Inter-Ministry Committee" (IMC), in relation to the NPO sector. Both reviews focused on the adequacy of laws and regulations that relate to the NPO sector. In particular, the 2004 review concentrated on the governance arrangements of IPCs and made extensive recommendations to improve those arrangements, including greater financial controls and accountability as well as mandatory disclosure requirements to the public. The 2006 review looked in detail at the regulatory arrangements of both charities and IPCs and made numerous recommendations to the government (which were accepted) to re-structure the regulatory framework to better enhance self regulation and governance of both entities.

786. In accordance with a recommendation by the IMC, the Commissioner of Charities and the six Sector Administrators (discussed below) are conducting independent governance reviews on large charities to assess and help improve their standard of corporate governance, financial control and regulatory compliance. This is the Commissioner's and Sector Administrators' role as part of the regulatory framework of the charity sector. To date, the Commissioner and Sector Administrators have also conducted the reviews of large charities and IPCs under their respective purview. Also, according to the Commissioner's web site, his office has conducted a number of other significant reviews of charities for a variety of reasons some of which relate to IMC recommendations.

787. Despite the details of these reviews, Singapore has not yet assessed the NPO sector to determine vulnerabilities, if any, to terrorist financing.

Protecting the NPO sector from terrorist financing through outreach and effective oversight

788. There have been a number of outreach initiatives conducted by the Commissioner of Charities to the charities sector as well as to the general public. These initiatives have included:

- Seeking public comment on and implementing the tightening of rules for the registration of charities to ensure only bona fide organisations are registered as charities.
- Establishing a "Charity Council" (chaired by the Chairman of Ernst and Young in her personal capacity) comprising 14 members to encourage the adoption of good governance standards and best practice to enhance public confidence in the charities sector.
- Developing, promoting and seeking public views on a Code of Governance for Charities in Singapore.

789. Moreover, the Commissioner has issued a publication referred to as "Anti-Money Laundering and Counter-Terrorism Financing" which alerts charities to Singapore's ML/FT laws; how to counter certain ML/FT risks within the sector; and reminds those entities of their obligations to file STRs to the STRO. According to the Commissioner, no charity or IPC has yet filed a STR. The Commissioner also works closely with specific government agencies in relation to AML/CFT.

790. All charities in Singapore are subject to some form of supervision. Responsibility for charities and IPCs rests with the Ministry of Community Development, Youth and Sports. All charities and IPCs operating in Singapore must register under the Charities Act – the Commissioner of Charities is the statutory supervisory authority. Under section 4 of the Charities Act, the role of the Commissioner is to:

- Maintain public trust and confidence in charities.
- Promote compliance by charity trustees with their legal obligations in exercising control and management of the administration of their charities.
- Promote the effective use of charitable resources.
- Enhance the accountability of charities to donors, beneficiaries and the general public.

791. Six government agencies (referred to as Sector Administrators) have been assigned to assist the Commissioner to oversee charities and IPCs within their individual mandate: the Ministries of Education, Health and Information, Communication and the Arts, as well as the National Council of Social Services, the People's Association, and the Singapore Sports Council. Charities and IPCs that do not fall under these sectors are supervised directly by the Commissioner.

792. Charities and IPCs are required to:

- Include information on the objects, activities and the charity trustees, as well their governing instrument when applying to the Commissioner.
- Submit an Annual Report to the Commissioner with statements of account.
- Submit annual accounts to the Comptroller of Income Tax who examines them to ensure they are within charitable spending limits (s.13M and 16, Income Tax Act).

793. Moreover, the names of charity trustees and their dates of appointment, the names, designations and dates of appointment of the management committee; and the names of the bankers, lawyers, auditors and investment advisors of the charity must also be disclosed. The Charity and IPC Annual Report to the Commissioner (required under s.16 of the Charities Act) is open to public inspection (s.17 Charities Act). Supplying false or misleading information is punishable as a criminal offence (s.10 Charities Act).

794. The Commissioner of Charities has the power to sanction violations of oversight measures including:

- Deregistration of a charity or IPC.
- Removal or suspension of any trustee, officer, agent or employee for misconduct or mismanagement.
- Establish a scheme for the administration of the charity or appoint a receiver or manager in respect of its property and affairs.
- Restrict transactions which may be entered into, or the nature or amount of the payments which may be made, in the administration of a charity without the Commissioner's approval.
- Vest charity property in the Public Trustee.
- Order any person holding property on behalf of the charity not to deal with it or any debtor not to make payment to the charity without the commissioner's approval (s.5, 24, 25, 25A, 26A and 26B, Charities Act).

795. The Charities Act was amended in March 2007 to give the Commissioner and the Sector Administrators greater powers to perform their role effectively, including the power to conduct governance reviews and investigations, act for the protection of charities and IPCs, and suspend public fund-raising by a charity where necessary (s.14, 25 and 39B, Charities Act; regulation 5, Charities (Registration of Charities) Regulations 2007). Recently (2 May 2007) the Commissioner exercised his power to de-register three charities on the grounds of serious irregularities in the administration of those charities by its Trustees.

796. All charities (other than exempt charities – *e.g.* Universities, hospitals etc under Schedule to the Charities Act) in Singapore must be registered with the Commissioner of charities within three months of their establishment. The Commissioner works with the Ministry of Home Affairs when vetting charity and IPC applications and when, in conjunction with this, conducting background checks on proposed trustees. The Commissioner advised that he would be advised by the MHA or other supervisory authorities if any trustee were on the UN 1267 list. The register of charities is open to public inspection (s.5 Charities Act).

797. Charities must keep accounting records sufficient to show and explain all the charity's transactions monies received and expended and a record of assets and liabilities. The accounting records must be kept for at least five years from the end of the financial year (s.12 and 13 Charities Act). Where a charity's gross income or expenditure exceeds SGD 250 000, the accounts must be audited by a public accountant (s.14 Charities Act). Large charities (with receipts of SGD 10 million in each of the last two financial years) must change their auditors at least once every 5 years, whether to another auditor from the same auditing firm or company or to another auditor from a different auditing firm or company (regulation 5, Charities (Large Charities) Regulations 2007).

798. The accounts and auditor's report must be attached to the annual report and submitted to the Commissioner and be publicly inspected (s.16 and 17, Charities Act). Any person can also obtain a copy of the charity's most recent accounts from the charity: Section 17 Charities Act. Larger charities (with receipts of SGD 10 million in the last two financial years) must have its accounts audited by an approved auditor (regulation 5, Charities (Large Charities) Regulations). The accounts are examined by the Commissioner and IRAS.

799. IPCs (which can raise funds from the public and issue receive tax deductible receipts) are subject to more stringent requirements. IPC accounting records must detail all donations received and disbursed and every tax-deductible donation must record the name of the donor, his identification number, the date and type of donation received (regulations 10 and 12, Charities (Institute of Public Character) Regulations). IPCs are required to disclose their financial data and profile information such as objectives, board members, programmes and activities on the internet website (regulation 19, Charities (Institutions of A Public Character) Regulations 2007). Where the fund-raising appeal is of

SGD 1 million or more, the details (income, expense and use of funds) must be disclosed on the internet website (regulation 14, Charities (Institutions of A Public Character) Regulations 2007).

Targeting and attacking terrorist abuse of NPOs through effective information gathering, investigation

800. There are a variety of mechanisms to secure information on charities and IPCs. For instance, under section 8 of the Charities Act, the Commissioner has the power to institute inquiries with regard to charities either generally or for particular purposes. These powers include the right to obtain information from charities and IPCs including accounts and copies of documents. There is also (under s.9) the right to question persons and take documents. It is an offence under the Act to furnish false information. According to the filed Annual Reports of the Commissioner on the Charities website, this inquiry power into specific charities has been used in a number of cases for a variety of purposes. Also, the Commissioner and Sector Administrators conduct regular field visits to, and governance reviews of, charities and IPCs. The Commissioner is currently conducting governance reviews of charities with SGD 10 million or more in income.

801. In addition to the powers of the Commissioner, law enforcement authorities (including officers from STRO and the Financial Investigations Branch) are able to access NPO information pursuant to existing working arrangements rather than the formal powers. Moreover, the regulatory framework of the Commission involving the six Sector Government Administrators within the purview of the Commissioner's remit creates an efficient mechanism to share information within a broad range of government agencies without the necessity of formal instruments.

802. Singapore has developed and implemented mechanisms for the prompt sharing of information among all relevant authorities in order to take preventative or investigative action when there is a suspicion or reasonable grounds to suspect that a particular NPO is being exploited for terrorist financing purposes or is a front organisation for terrorist financing. Section 8 and 10 of TSOFA imposes duties upon all persons including charities and IPCs in Singapore (in the case of s.10) and Singapore citizens outside of Singapore to disclose to a police officer any information regarding possession, custody or control of terrorist property, on a terrorist transaction in respect of any property belonging to terrorist or terrorist entity or about acts of terrorism financing.

Responding to international requests for information about an NPO of concern

803. For international cooperation issues in relation to suspected FT or other forms of terrorist support, the Singapore Police, including STRO, as the primary point of contact for incoming and outgoing requests from foreign counterparts.

5.3.2 Recommendations and Comments

804. A central registration system exists under the Charities Act for the NPO sector in Singapore. The Commissioner of Charities, with six government Sector Administrators to coordinate information, is an efficient and well-structured system for oversight of this sector. Violations of obligations may be sanctioned by the Commissioner. The Commissioner's Annual Reports published on the web site of the Commissioner indicate that such action is in fact taken for a variety of reasons.

805. The Commissioner should conduct a TF vulnerability review of the NPO sector. Although Guidance on TF risks, as well as ML risks, has been published widely to the sector with suggestions on how to mitigate that risk. The Guidance should be accompanied by outreach to the sector either by the Commissioner or through the Sector Administrators with further and more detailed information.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**LC**	• Singapore has not yet conducted a TF vulnerability review of the NPO sector.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National Co-Operation and Coordination (R.31 & 32)

6.1.1 Description and Analysis

Recommendation 31 (Domestic co-operation)

Policy co-operation

Steering Committee

806. Singapore utilises a multi-agency AML/CFT strategy involving law enforcement, policy makers, regulators and the private sector. This effort is led by a high-level Steering Committee established in 1999 and is comprised of the Permanent Secretary of the Ministry of Home Affairs (PS(HA)), the Permanent Secretary of the Ministry of Finance (PS(F)) and the Managing Director of MAS. The Steering Committee centralises decision-making and communication. It also aims to ensure that agencies have effective mechanisms in place to enable them to cooperate and, where appropriate, coordinate domestically with each other concerning the development and implementation of AML/CFT policies and activities.

Inter-Agency Committee

807. The Steering Committee is supported by the working-level Inter-Agency Committee (IAC) that was established in 1993 and is currently comprised of the following 15 agencies that play a role in AML/CFT:

(a) **Ministry of Home Affairs (MHA)** is the lead agency in the AML/CFT effort and oversees law enforcement and security matters.

  (i) **CAD** is the main enforcement agency for money laundering and comes under the MHA. Singapore's financial intelligence unit (the STRO) is a unit within the CAD.

  (ii) **Central Narcotics Bureau** is responsible for the seizure of drug assets and comes under MHA.

(b) Ministry of Law (MinLaw) and Attorney General's Chambers (AGC) ensure that Singapore has a clear legal infrastructure in relation to ML/FT matters).

(c) Monetary Authority of Singapore (MAS) is Singapore's single regulator for financial sectors, including the banking, securities insurance and trust companies sectors, and oversees AML/CFT matters in the financial industry.

(d) Corrupt Practices Investigation Bureau (CPIB) comes under the Prime Minister's Office, and enforces Singapore's AML legislation in relation to corruption.

(e) Accounting and Corporate Regulatory Authority (ACRA).

(f) Ministry of Finance (MOF).

(g) Magilis Ugama Islam Singapura, also known as the Islamic Religious Council of Singapore (MUIS).

(h) Ministry of Community Development, Youth and Sports (MCYS).

(i) Ministry of Trade and Industry (MTI).

(j) Standards, Productivity and Innovation Board (SPRING).

(k) Singapore Land Authority (SLA).

(l) Ministry of Foreign Affairs (MFA).

808. The IAC meets several times a year (formally or informally) and corresponds very frequently over email to coordinate and improve Singapore's AML/CFT regime. This forum provides the opportunity for sharing of information, and coordination of policy decisions and implementation issues between key relevant competent authorities. Singapore strives to keep pace with the developments on AML/CFT, by seeking agencies' responses to FATF typologies and circulating best practice papers. Part of the IAC's work is to get agencies actively involved in managing and mitigating new ML/FT threats. The IAC will also propose recommendations to the high-level Steering Committee for policy directions. The Singaporean authorities report that there is excellent co-operation between agencies as well as among financial institutions and law enforcement agencies.

Inter-Ministry Committee on Terrorism (IMC On Terrorism)

809. To ensure a coordinated effort in combating terrorism (including terrorist financing), members of the IAC are also represented on the Inter-Ministry Committee on Terrorism (IMC On Terrorism). The IMC was established in 2001 under the AGC, MFA and MinLaw to ensure Singapore's full compliance with international obligations, and to strengthen its national capacity to combat international terrorism. The Committee comprises all agencies on the IAC, as well as the Ministries of Defence, Foreign Affairs, Transport, and Trade and Industry. IMC's primary emphasis is to coordinate the effective implementation of Singapore's international obligations with respect to the combating of terrorism.

810. The members of the IAC and IMC frequently work together to ensure a consistent and coherent approach in Singapore's AML/CFT strategy, and can extend their membership to other Ministries if there are pertinent issues that would involve these other agencies. Policy decisions made at the IAC and IMC level are submitted for concurrence to the Steering Committee/ministerial level. The policies decided at the Steering Committee/ministerial level then cascade downwards through the respective agencies for implementation.

National Security Coordination Secretariat (NSCS)

811. The National Security Coordination Secretariat (NSCS) was formed in 2004 to fight the threat of terrorism. It is headed by the Coordinating Minister for National Security and is comprised of the National Security Coordination Centre and Joint Counter Terrorism Centre. The NSCS works closely with the members of the IMC to ensure a co-ordinated fight against terrorism and terrorist financing.

Ad hoc groups

812. When necessary, ad hoc groups dealing with specialised issues are formed to study the issues in detail before formulating a policy position for consideration. The special groups have included the task forces set up to study the amendments to the TSOFA and the CDSA for greater compliance with the international standards (including those of the FATF) as well as the implementation of Special Recommendation IX in Singapore. The members of these ad hoc groups include the policy and operational staff from the relevant agencies and may also comprise subject matter experts.

Operational co-operation:

Coordination of ML/FT investigations

813. Established protocols and working arrangements are also in place to maximise the investigative efforts of the agencies. Additionally, the AGC must concur before any ML/FT prosecution can be proceeded upon (in accordance with s.58, CDSA). The concurrence must be processed by the AGC. This helps to ensure that there is a clear delineation of responsibilities in the investigation. This control system also ensures a high quality of investigation and prosecution.

814. In relation to money laundering investigations, the authorised officers from the respective agencies derive their powers from the CDSA as well as other empowering legislation such as the CPC generally. The officers from the CNB also derive their powers from the MDA and the CPIB, from the PCA. In cases where there is an overlap of jurisdictions, the matter of the appropriate investigative agency is discussed between the various Directors of the respective agencies to prevent duplication of efforts. CNB and CAD have a long-standing working arrangement in which the roles of the respective agencies are clear. The FIB is the main investigative agency to review any money laundering offence, and only refers the matter to another appropriate agency if such an agency can be identified. Both the FIB and the PCU work closely within the SPF and report directly to AD FID. AD FID, who participates in the IAC, also reports to the Senior Deputy Director and Director of CAD with a view to ensuring that all ML investigations are handled promptly and effectively. It also works closely with CNB and CPIB to ensure that there will be no overlapping of efforts. Additionally, it is possible for the investigative agencies to work together towards the conclusion of a money laundering investigation.

815. In relation to terrorist financing investigation, the FIB works closely with security agencies on matters relating to national security, including terrorism related matters.

Coordination of internal security issues

816. The Ministry of Home Affairs is the agency in charge of the internal security of Singapore. Other agencies under MHA include:

(a) Singapore Police Force (SPF).

(b) The Internal Security Department.

(c) The Singapore Civil Defence Force.

(d) The Prisons Department.

(e) Immigration & Checkpoints Authority.

(f) Central Narcotics Bureau (CNB).

(g) Singapore Corporation of Rehabilitative Enterprise.

817. Together these agencies formed the Home Team of Singapore, which encourages the agencies to work closely together. This has provided effective synergy in national cooperation.

Operational Coordination and Meetings

818. CAD has regular coordination meetings with CPIB, CID, ISD and other members of the IAC, both at the working and management level to allow the agencies to keep each other abreast of the latest developments in their own respective areas of competence. In one case, the CAD collaborated jointly with CPIB to examine both the corrupt and money laundering aspect of a case involving a publicly listed company. Coordination between the agencies also includes informal exchanges between the line officers of the enforcement agencies. This can also take the form of intelligence coordination.

Intelligence (Intel) Coordination and Meetings

819. As STRO is part of the police force, it is able to maintain a very good working relationship with the enforcement units, particularly the specialised branches dealing with money laundering and terrorism financing (*i.e.* FIB and PCU). STRO has frequent meetings with other agencies in the intelligence community to seek to enhance the existing level of cooperation. STRO has assisted in the detection of unlicensed money lending syndicates in Singapore etc. STRO also shares with the relevant agencies any emerging trends and typologies that it has observed in the course of its work. STRO also conducts regular meetings to share information with the various investigative agencies in Singapore including enforcement units within CAD, CID (*e.g.* Gambling Suppression Branch and Anti-Unlicensed Money Lending Unit), CPIB, CNB, IRAS, Customs, etc.

820. In terms of coordination and information sharing, law enforcement agencies such as the CAD provide a major source of intelligence. CAD relies on the STRs produced by the reporting entities and the AML/CFT regime to perform their investigations and for the gathering of information for typologies work. MAS also has intelligence capability, by virtue of understanding the threats facing the Singapore's financial system and identifying areas of poor performance in the industry. This information gathered by agencies is shared with each other and with the industry (through its publication such as the Reports from STRO, CAD/STRO Annual Report 2007, Bulletins in STROLLS etc.) and at the IAC and IMC meetings. Examples of close working relationships include the attachment of two Deputy Public Prosecutors from the AGC at any one time to the CAD and the regular formation of inter-agency delegations to participate in meetings of the FATF and the Asia-Pacific Group on Money Laundering (APG).

Additional elements

821. The members of the IAC also meet and coordinate with the members of the regulatory agencies, including MAS (Financial Sector), LawSoc (Lawyers and Notaries Public), Casino Regulation Division (Casinos), ACRA (Companies Service Providers), ICPAS (Accountants), SPRING Singapore (Jewellers), Singapore Land Authority (Real Estate) etc. These meetings are coordinated by MHA/MAS. STRO has also increased its efforts to reach out to the DNFBPs, including by liaising with the regulatory bodies such as LawSoc, ACRA, Casino Regulation Division, SPRING Singapore etc.

Resources of policy makers

822. The Steering Committee, to which the IAC reports, would, if necessary, deal with resource planning issues at a national level between agencies, through recommendations from the IAC. In general, however, each agency represented on the IAC is responsible for putting in place appropriate recruitment practices that ensure the integrity as well as technical ability of its staff. The priority given to AML/CFT issues is demonstrated in the allocation of adequate resources within each agency for the purpose of reviewing policy and carrying out supervisory and enforcement activities. The key agencies that participate in policy decisions are required to maintain high professional integrity standards, including standards concerning confidentiality, and are of high integrity and appropriately skilled. See sections 2.5, 2.6 and 3.10 of this report for more details.

823. Policy officers dealing with AML/ CFT at the Ministry of Home Affairs attend specific AML/ CFT courses, for example, the "Anti-Money Laundering/Counter Financing of Terrorism Conference", jointly organised by the Commercial Affairs Department and Internal Security Department, and the "Seminar on Mutual Legal Assistance in Criminal Matters: Policies, Principles, Practices", organised by the Attorney-General's Chambers as well as the Financial Crimes Conferences jointly organised by the public and private sectors. Policy officers have also participated in FATF training courses, such as the FATF assessor training, and regularly attend FATF Plenary and working group meetings. In addition, policy officers also receive training in generic areas such as policy formulation and legislative drafting.

Recommendation 32 (Reviewing the effectiveness of AML/CFT systems)

824. Agencies maintain statistics on matters relevant to the effectiveness and efficiency of AML/CFT systems. This includes the statistics on the STRs received and disseminated; on ML/FT investigations, prosecutions and convictions; and on international legal assistance and cooperation. The Steering Committee uses these statistics in discussions with relevant agencies to direct them to review the effectiveness of their AML/CFT systems.

825. The IAC is responsible for reviewing the effectiveness of Singapore's AML/CFT system. The working group meets on a regular basis to review the system's effectiveness as well as to discuss new initiatives to strengthen Singapore's AML/CFT system. Ad hoc committees also submit their findings for consideration at the IAC. The risk assessment of the vulnerability of the various sectors and the specific industry/professions would also be considered by the working group, and the appropriate recommendations made. The recommendations made by the working groups are then submitted to a high level Steering Committee for consideration and approval. Policy considerations at the Ministerial level would also be sought through the Steering Committee. Pursuant to this system of review, Singapore has made various improvements to its AML/CFT regime, including amendments to legislation (such as the CDSA and TSOFA), expanding the powers of the FIU, and extending AML/CFT requirements to accountants, lawyers and trust companies.

6.1.2 Recommendations and Comments

826. Singapore authorities have adequate and effective mechanisms for domestic co-ordination and co-operation, both at the policy and operational levels. This Recommendation is fully compliant.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**C**	This Recommendation is fully observed.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

827. Singapore is a party to the Vienna Convention, having acceded to it on 21 October 1997, and it entered into force with respect to Singapore on 21 January 1998. Singapore has implemented the vast majority of the convention's provisions; however, the purposive elements required to prove third party money laundering are not in line with the convention.

828. Singapore is also a party to the Terrorist Financing Convention (TFC), having ratified it on 30 December 2002. It entered into force with respect to Singapore on 29 January 2003. The majority of the provisions have been implemented; however, the scope of "terrorist act" does not fully cover all of the acts defined in Article 2(1).

829. Singapore signed the Palermo Convention on 13 December 2000 and deposited its instruments of ratification with the UN on 28 August 2007. It entered into force with respect to Singapore on 27 September 2007. While Singapore has implemented the majority of the convention's provisions, the purposive elements required to prove third party money laundering are not in line with the Convention's ML articles.

830. ***S/RES/1267(1999) and successor resolutions:*** While Singapore generally implements these resolutions effectively, provisions for obtaining access to frozen funds to pay basic expenses should be made specifically subject to the requirement of obtaining approval of the 1267 Committee for funds or other assets frozen as a result of S/RES/1267(1999).

831. ***S/RES/1373(2001):*** Singapore generally implements the requirements in S/RES/1373(2001) effectively. Although Singapore relies on its well-honed procedures of advising its ministries and regulatory bodies of MHA's decisions to give effect to the actions initiated under the freezing mechanisms of other jurisdictions, or to designate persons in the context of S/RES/1373(2001), there is not a particularized legal framework for doing so. In addition, S/RES/1373 also requires countries to fully implement the CFT Convention – while the majority of the Convention's provisions have been implemented, the scope of "terrorist act" does not fully cover all the acts defined in Article 2(1). Also, there is no formal de-listing procedure in place. See section 2.4 of this report for details.

Additional elements

832. As a Southeast Asian country, Singapore has no automatic right to accede to the 1990 Council of Europe Convention and the 2002 Inter-American Convention. These are Conventions applicable to a different geographical region and thus irrelevant for Singapore.

6.1.2 Recommendations and Comments

833. Singapore should amend its money laundering and terrorist financing offences to be fully consistent with the international Conventions (Vienna, Palermo, FT Convention).

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**LC**	• The purpose elements required to prove third party money laundering are not in line with the Vienna and Palermo Conventions. • The scope of "terrorist act" does not fully cover all of the acts defined in Article 2(1) of the FT Convention.
SR.I	**LC**	• The scope of "terrorist act" does not fully cover all of the acts defined in Article 2(1) of the FT Convention. • Provisions for obtaining access to frozen funds to pay basic expenses should be made specifically subject to the requirement of obtaining approval of the 1267 Committee for funds or other assets frozen as a result of S/RES/1267(1999) • The measures to implement S/RES/1373(2001) suffer from the following deficiencies: - Although Singapore relies on its well-honed procedures of advising its ministries and regulatory bodies of MHA's decisions to give effect to the actions initiated under the freezing mechanisms of other jurisdictions, or to designate persons in the context of S/RES/1373(2001), there is not a particularized legal framework for doing so - While the majority of the FT Convention's provisions have been implemented, the scope of "terrorist act" does not fully cover all the acts defined in Article 2(1).

6.3 Mutual Legal Assistance (R.36-38, SR.V, R.32)

6.3.1 Description and Analysis

Recommendation 36 and SR.V

834. The mutual legal assistance provisions described below are implemented and apply in exactly the same way in relation to foreign criminal investigations involving ML, FT and predicate offences.

835. The Mutual Assistance in Criminal Matters Act (MACMA) allows Singapore to provide mutual legal assistance to other jurisdictions, in relation to criminal investigations or criminal proceedings for offences that are covered under the Act. As of 1 November 2007, a total of 335 crimes are covered under the MACMA, including ML and TF, for which assistance may be rendered to a

requesting State in relation to a corresponding foreign offence. The 335 offences covered by MACMA are listed in the Schedules 1 and 2, CDSA.[96]

836. The issue of international requests for financial (bank account) information has been the crucible of foreign requests for mutual legal assistance from Singapore. The reason for this is that financial information cannot be provided to foreign authorities through informal channels, or without a High Court order. At present, Singapore's FIU cannot make financial information available to its foreign counterparts, except to the extent the information is contained in an STR, and bank account information may only be obtained from Singapore with a formal request for mutual legal assistance under the MACMA. Section 22(2) of MACMA requires that the AGC obtain an order by the High Court for such information. This is the only category of information that is treated in this fashion.

Range of mutual legal assistance provided

837. There are generally clear and efficient processes in place for the execution of MLA requests in a timely way and without undue delays. There are process flowcharts, standard operating procedures on mutual legal assistance, timeline requirements and monitoring mechanisms for processing MLA requests. Internally, enforcement agencies such as the CAD, has also developed their own set of internal guidelines, consistent with the approach of AGC, in handling requests for assistance.

838. For a number of years, Singapore's only mutual legal assistance agreements with other countries covered drug offences. In April 2006, the MACMA was amended to provide a bilateral case-by-case initiative that would be available to all countries in all instances in which Singapore and the foreign government would agree to provide the same type of assistance in a similar reciprocal request. This statute appears to remedy many, but not necessarily all, of the problems that existed previously, specifically the requirement for an *ex parte* hearing and court order to obtain financial records and information.

839. Under the MACMA, so long as the foreign requesting government is able to undertake a mutual assistance reciprocity agreement, on a case-by-case basis, Singapore is now able to render foreign jurisdictions assistance such as recording of evidence in Singapore for the purpose of pending criminal proceedings in a foreign country, the service of foreign process in Singapore in connection with a criminal matter in a foreign country, and the location of persons in Singapore for drug offences and all "serious offences" under Singapore law (which includes the CDSA Schedule 2 listed offences). Since 1 April 2006, an MLAT is no longer required before coercive assistance can be provided to any requesting State (*e.g.* orders for compelling the production of information or records, arranging for a witness in Singapore to give evidence in a foreign country, the enforcement of foreign confiscation orders, and requests for search and seizure) as long as the requesting State provides a reciprocity undertaking before assistance is granted.

840. Singapore has had bilateral MLATs with the Hong Kong Special Administrative Region since 2004 and with India since 2005. Singapore also has had a bilateral MLAT in the form of a Drug Designation Agreement in force with the United States since 2000. Singapore also has had a treaty relationship with four Southeast Asian States, namely Malaysia, Vietnam, Brunei Darussalam, and Laos, as all four countries have ratified the 2004 regional Treaty on Mutual Legal Assistance, which was signed by the 10 ASEAN countries.

841. Currently, under MACMA, Singapore can render assistance to any requesting State that has been designated as a "prescribed foreign country". Under section 17(1) MACMA, the Minister for Law may declare a foreign country a prescribed foreign country if there is in force a treaty, memorandum of understanding or other agreement between Singapore and that country under which that country has agreed to provide assistance in criminal matters to Singapore. Currently, the following countries are "prescribed foreign countries" under section 17 MACMA: US (drug and terrorism

[96] Amendments to the CDSA, effective 1 November 2007, added 36 offences to the First and Second Schedules.

financing offences), UK (terrorism financing offences), the Hong Kong SAR, Malaysia, India, the Socialist Republic of Vietnam, Brunei Darussalam and the Lao People's Democratic Republic.

842. Under section 16(2) of MACMA, assistance may also be provided to a foreign country that is not a prescribed foreign country if the appropriate authority of that country gives a reciprocity undertaking to the AGC. Once such an undertaking is provided, the AG may proceed to process the request and provide the assistance sought. The undertaking is usually worded specific to the offence in relation to that particular request and head of assistance sought. Examples of countries that have been deemed prescribed foreign countries pursuant to this provision include: the UK, Australia, Italy, Switzerland and the US. When a subsequent mutual legal assistance request is made which is unrelated to the first request, a separate undertaking will have to be given, as the offences, facts and assistance sought may be different.

843. Assistance that may be provided includes the production or seizure of information, documents, or evidence (including financial records) from financial institutions, other entities, or natural persons; and searches of financial institutions, other entities, and domiciles (MACMA s.22 (1) and (4), and s.33). MACMA also provides for the obtaining of sworn witness testimony, as well as the identification, freezing, seizure, or confiscation of assets laundered or intended to be laundered, the proceeds of ML and assets used for or intended to be used for FT. MACMA also does not preclude assistance being rendered on an informal basis if the subject of the request consents. Witness testimony and certain forms of non-coercive assistance – such as locating persons and/or public information, may also be provided to non-prescribed countries (MACMA s.21, 27(1), 37 and 38).

844. ML offences in sections 44 and 47 of the CDSA are serious offences under the CDSA Second Schedule of 329 serious crimes, and are, therefore, also considered "serious offences" for MACMA purposes, as are TSOFA terrorist or terrorist financing offences (CDSA, Second Schedule, s.278-281). In addition, section 32 of TSOFA provides that all parties to the TF Convention are deemed prescribed parties for the purposes of Singapore rendering assistance under MACMA, and that assistance shall not be refused on the basis of such offences being political in nature.

845. Singapore authorities maintain that MACMA has enabled them to provide mutual legal assistance (MLA) in a timely, constructive and effective manner. Requests for MLA are processed by the AGC, as the Attorney-General is designated as the Central Authority for such requests. The AGC has a set of standard operating procedures, including a set of standard forms, to deal with and facilitate such requests. These documents are available to officials from other countries on the AGC's website, and are presented in a user-friendly format. According to the AGC, current processing time for a simple MLA request ranges from two to four weeks, while a more complex request may take a few months or more to process given the need to seek clarifications and requisite undertakings from the requesting State. Authorities state that urgent applications for MLA request are processed on a priority basis to ensure that the information or evidence sought can be forwarded to the requesting State within the time requested by the latter once the request is granted. Statistics provided by the AGC indicate that average turnaround time for MLA requests during 2004 and 2005 was 4.5 to 4.8 months. That figure dropped to 3.5 months in 2006, and with the enactment of the MACMA amendments, diminished to 1.5 months through July 2007.

846. Singapore authorities concede that some requests made before 1 April 2006 (when the MACMA amendments came into force) were rejected because they sought coercive measures (such as production orders or confiscation orders) which could not be extended in the absence of an MLAT at that time. Singapore maintains that with the 2006 amendments to MACMA, there is now greater flexibility for assistance of the type contemplated by FATF that may be rendered on a case-by-case basis to countries with which Singapore has no MLAT. These provisions also apply to foreign requests for assistance on terrorist and terrorist financing cases. According to the AGC, 3 requests for MLA for terrorist-related offences were made and granted during 2004 and 2005. One such request, made in 2007, is pending.

Prohibitions and conditions

847. The MACMA contains 12 mandatory grounds of refusal, including requests of a political character and based on a person's race, religion, nationality, etc, and dual criminality (section 20(1), and 4 discretionary grounds of refusal (s.20(2)). The Singaporean authorities note that the most commonly invoked grounds of refusal is that the foreign offence in question does not correspond to one or more of the 335 scheduled offences in the CDSA list (First and Second Schedule), and the need for reciprocity undertaking from the requesting State. The other grounds of refusal are rarely invoked. Assistance is not refused on the basis that judicial proceedings have not been commenced in the requesting country (except possibly for requests for freezing/confiscation of assets). Where foreign criminal judicial proceedings "have been or are to be initiated in that country," the country may request the AGC to assist in freezing property located in Singapore which may become subject to a foreign confiscation order (s.29(b) MACMA). A conviction is also not required before restraint/seizure assistance may be provided, save for the enforcement of foreign confiscation orders.

848. Reciprocity and dual criminality are not interpreted in an overly strict manner as it is the criminal conduct alleged which is examined as a whole to determine whether the conduct would amount to a scheduled offence in the CDSA list in Singapore, not the label of the offence or its constituent elements that must match a scheduled offence in Singapore. The same provisions apply for TSOFA-type offences (*i.e.* terrorist financing offences).

849. As long as a request involves a foreign offence that can come within the scheduled CDSA list of offences if committed in Singapore, assistance will not be refused even if the offence can be described as one which involves fiscal matters. For example, in a 2006 case, a request that originated from a foreign tax authority essentially concerned tax evasion. However, as there was possibly forgery and cheating involved which resulted in the tax fraud, Singapore was willing to render assistance and to this end, sought further information from the requesting country concerning the forgery and cheating offences with a view to processing the request favourably.

850. Section 23(4) excludes items subject to legal privilege, which includes for example communications between an advocate/solicitor and client made in connection with the giving of legal advice or in connection with judicial proceedings. Otherwise, there are no grounds of refusal in MACMA that permits the refusal of assistance on the basis of secrecy or confidentiality, including financial secrecy requirements. Section 23(4)(b) of the MACMA expressly provides that a production order under section 22 of the MACMA shall have effect notwithstanding any obligations as to secrecy or other restrictions upon the disclosure of information imposed by statute or otherwise on the disclosure. Any person who complies with an order made under section 22 of the MACMA shall not be treated as being in breach of any restriction upon the disclosure of information or thing imposed by law, contract or rules of professional conduct (s.24(2) MACMA). Although Singapore does not refuse MLA requests for bank account information based on secrecy or confidentiality requirements placed on financial institutions, the procedures for obtaining such information are more extensive than for other types of information relevant to criminal investigations.

Powers of competent authorities when executing mutual legal assistance requests

851. Section 22 of the MACMA provides that where a request is made by the appropriate authority of a foreign country that any particular thing or description of thing in Singapore be produced for the purposes of any criminal matter in that country, the Attorney-General or a person duly appointed by him may apply to the court for a production order. All of the investigative/law enforcement powers available to the authorities in domestic matters can be used in mutual legal assistance matters. Please see section 2.6 of the report for more details.

Conflicts of jurisdiction

852. If and when a situation regarding a conflict of jurisdiction were to arise in cases that are subject to prosecution in more than one country, the Singaporean authorities advise that they will discuss with the relevant foreign country or countries to decide on the most appropriate venue for prosecution of defendants in the interests of justice. However, Singapore has yet to come across such a conflict of jurisdiction situation.

Additional elements

853. In relation to both ML and FT, information obtained as a result of the exercise of such powers (including coercive powers) by local enforcement agencies can be shared with foreign counterparts on an intelligence basis. The exception to this is that Singapore police have indicated that sometimes they will obtain financial information under their police powers (CPC s.58(1). However, without a domestic investigation pending, officers cannot share that information with their foreign counterparts. Also, STRO may not share bank information with foreign counterparts unless the information is contained in an STR. Formal requests for assistance are required. Customarily, if informally presented information is required to be presented formally (*e.g.* by affidavit), then either the consent of the provider will be required (*e.g.* a witness' statement) or a court order will be needed (e.g. production of records held by a financial institution). In such a case, a formal request to the Central Authority (designated to be the AGC) will be required.

Recommendation 37 (dual criminality relating to mutual legal assistance)

854. Dual criminality, in the sense that the foreign offence in question must correspond to one of the scheduled 335 offences in the CDSA list (First or Second Schedule), is a requirement for assistance of the type contemplated (s.20(1)(f), MACMA). The provisions of MACMA only deal with requests for assistance for coercive measures. In that sense, dual criminality is a mandatory requirement for the specific types of assistance laid out in the act (s.20(1)(f) MACMA). However, the rendering of assistance to foreign States of a type not covered within the scope of MACMA is not precluded (s.4 MACMA). For such types of assistance, *i.e.* non-coercive measures, the requirement of dual criminality can be dispensed with.

855. According to Singapore authorities, dual criminality requirement is not interpreted strictly, but in a holistic manner. In such cases, a purposive rather than a literal interpretation is adopted. Dual criminality is made with reference to an offence against the law of, or of a part of, a foreign State and the act or omission constituting the offence or the equivalent act or omission would, if it took place in or within the jurisdiction of Singapore, constitute an offence against the law in force in Singapore in accordance with scheduled 335 offences. Examination is made on the underlying conduct as a whole, and not based on the label or elements of the offence in the foreign State.

Recommendation 38 and SR.V (MLA – Freezing, seizing and confiscation)

856. Section 29 of the MACMA provides that the appropriate authority of a foreign country may request the Attorney-General to assist in:

(a) The enforcement and satisfaction of a foreign confiscation order, made in any judicial proceedings instituted in that country, against property that is reasonably believed to be located in Singapore (including laundered property from a relevant predicate offence listed in the Schedules 1 and 2, CDSA or terrorist funds). Or

(b) Where a foreign confiscation order may be made in judicial proceedings which have been or are to be instituted in that country, the restraining of dealing in any property that is reasonably believed to be located in Singapore and against which the order may be enforced or which may be available to satisfy the order.

857. Upon receiving such a request, the Attorney-General may apply to the High Court for a restraining order or the registration of a foreign confiscation order. The High Court may, on such application, register the foreign confiscation order if it is satisfied (a) that the order is in force and not subject to further appeal in the foreign country; (b) where a person affected by the order did not appear in the proceedings, that the person received notice of the proceedings in sufficient time to enable him to defend them; and (c) that enforcing the order in Singapore would not be contrary to the interests of justice.

858. MACMA's definition of "foreign confiscation order" (s.2(1) includes an order based on the value of criminal payments or rewards accrued to a defendant, or property derived, directly or indirectly, from those payments or rewards; and, it also includes "an instrumentality order." However, MACMA's definition of "instrumentality order" applies only to drug cases, and not to other serious crimes. Nor does it include any instrumentalities "intended for use" in FT, ML, or predicate offences. As previously noted in section 3 of this report, Singapore's domestic CDSA provisions also do not permit restraint or confiscation based for instrumentalities or intended instrumentalities. Singapore authorities cite the police powers act, the CPC, for their authority to seize and forfeit instrumentalities.

859. For example, under s 68 CPC, the Police can, inter alia, *seize property which is found under circumstances which create suspicion of an offence*. The language of this provision should be wide enough to encompass the seizure of instrumentalities used in, or intended to be used, in the commission of such offences. In most cases, the presence of such instrumentalities in Singapore, coupled with the reliable information the Police receives from foreign counterparts would invariably disclose a domestic offence and allow the domestic powers under the CPC to be invoked. Such instrumentalities can subsequently be forfeited pursuant to the wide powers under s 386 CPC. Given the scope of Singapore's abetment provisions which would allow for a domestic investigation in most cases where instrumentalities are present in Singapore, this would mean that the CPC provisions can be invoked in most cases. However, these provisions would not assist foreign governments, unless Singapore opens its own domestic investigation in the matter. And, in cases where these provisions cannot be used, Singapore will likely insist that the sec. 29(b) MACMA prerequisites that criminal proceedings are about to be or have been filed by the requesting state be demonstrated.

860. In most cases where instrumentalities are located in Singapore, the Singaporean authorities do not foresee difficulty in opening such domestic investigations. In any event, Singapore has not received any requests from foreign governments to seize and forfeit instrumentalities; however, if such was received and a domestic investigation was not opened, assistance could not be provided, which renders the regime ineffective. In addition, as indicated under the discussion of Recommendation 3, the domestic provisions do not cover instrumentalities of corresponding value.

861. Under section 29(2) of the MACMA, the Attorney-General may register and enforce the foreign confiscation order upon receipt of a request for enforcement of foreign confiscation order or a request for restraining of dealing in property against which a foreign confiscation order may be enforced. A foreign confiscation order is defined in section 2(1) of the MACMA as an order by a court in a foreign country for the recovery, forfeiture or confiscation of: (1) payments or other rewards received in connection with an offence against the law of the country or the value of such payments or rewards, or (2) property derived or realized, directly or indirectly, from payments or other rewards received in connection with such an offence, or the value of such property. Thus, the equivalent value of payments or rewards may be confiscated, but not the equivalent value of instrumentalities.

862. As discussed above, the appropriate authority of a foreign country may request Singapore to assist in the restraint of criminal proceeds, or its equivalent value, under sections 29-32 of MACMA. In 2005, the first restraining order issued under MACMA was entered against funds in a Singapore bank account that constituted the proceeds of illicit internet pharmaceutical sales. The restraining order was timed to coordinate with the arrests of the defendants in other jurisdictions. Later, a production order was also obtained for bank accounts, which were provided to a foreign government.

863. Under section 33(1) of the MACMA, the appropriate authority of a foreign country may also request Singapore to assist in seizing any items for evidentiary purposes, or items which are otherwise "relevant to" the criminal matter, such as items purchased through fraud or theft.

Asset forfeiture fund and sharing of assets

864. Assets confiscated under the CDSA are placed in a Consolidated Fund administered by the Ministry of Finance unless the proceeds are being returned to identifiable victims. Funds in the Consolidated Fund are used for government expenditures, which would include law enforcement, health and education. Singapore has also considered establishing a separate asset forfeiture fund but has elected to manage confiscated assets without the use of such a fund. Singapore has indicated that it has experienced no difficulties in international sharing by not having a separate fund. Sharing of confiscated or forfeited assets (including those derived from investigations of ML, FT or predicate offences) with other countries when confiscation is directly or indirectly a result of co-ordinated law enforcement actions is possible under the Schedule of the MACMA, and these provisions have been used.

Additional elements

865. Foreign non-criminal confiscation orders (including those for ML, FT or predicate offences) may be enforced on a case by case basis under MACMA. However, Singapore law (except for the TSOFA) still requires that judicial proceedings (see paragraph 6 of the Schedule to the MACMA) be initiated in order for restraint to occur, and that a non-appealable final confiscation order be obtained before enforcement in Singapore can occur.

Resources (Central authority for sending/receiving mutual legal assistance/extradition requests)

866. Requests for mutual legal assistance and extradition are centrally dealt with by the Advisory Directorate of the AGC, which is headed by a Senior State Counsel and staffed by 7 experienced prosecutors. For full details of the AGC, including structure, funding, and staffing, see section 2.6 of this report.

867. In 2006, the Criminal Justice Division conducted a course for more than 100 participants including judges, prosecutors, officers of policy making agencies and law enforcement officers on mutual legal assistance (MLA) and extradition. A substantial component of the course was on ML and FT offences, within the broader context of MLA and extradition. Various case studies were examined to consider the practical and operational challenges involved in the investigations and prosecutions of ML and FT offences and relevant court applications for tracing, freezing, confiscation and forfeiture of assets. The course was over-subscribed and very well received and there are plans to repeat such training on a regular basis for additional details concerning the training of AGC staff, see section 2.6 of this report.

Statistics and Effectiveness

868. The AGC maintains annual statistics on all MLA and extradition requests, including requests relating to the freezing, seizing and confiscation of assets that are made or received from foreign governments. These figures are further broken into requests relating to ML, the predicate offences and FT. Statistics cover the nature of the request, whether it was granted or refused, and the time required to respond. Statistics on the total number of incoming and outgoing MLA requests and extradition requests from the period 1 January 2004 to July 2007 is provided in the table below.

	2004	2005	2006	2007 (up to July)
Outgoing requests	1	2	2	0
Incoming requests [97]	64	53	63	49
Incoming requests by Heads of Assistance	86	85	110	69
Acceded Requests	31	18	20	16
Rejected Requests	16	12	10	9
Partially Acceded Requests[98]	5	7	5	1
Withdrawn Requests	4	2	4	2
Pending Requests	1	2	17	21
Requests deemed lapsed[99]	7	12	7	0
Requests for ML offences	3	9	8	6
Requests for other offences Fraud/ Cheating/CBT/Misappropriation/ Forgery Corruption	62[100] 26 3	44[101] 27 1	56[102] 18 2	43[103] 11 2
Average turnaround time[104]	4.5 months	4.8 months	3.5 months	1.5 months
Requests for terrorist related offences[105]	2	1	0	1
Status	Acceded	Acceded		Pending

869. These statistics indicate that the turnaround time for Singapore's response to international requests has, indeed, shrunk since MACMA came into effect in 2006. However, they do not indicate any appreciable increase in the number of requests to which Singapore acceded, despite the fact that the MACMA widened the scope of criminal offenses for which mutual legal assistance could be granted, and there are a large number of incoming requests still pending, despite the lowered turnaround time. Thus, there is still clearly room for improvement in positively responding to requests. Also, the low number of outgoing requests appears to be further indicative of Singapore's decision not to concentrate on investigating foreign predicate crimes which may be responsible for some funds on deposit in Singapore's financial sector.

870. Several countries have indicated that, before the passage of the 2006 MACMA amendments, Singapore would not render coercive assistance, including the provision of bank records and financial information, without having an MLAT, of which there were few. In addition, countries indicated long

97 Includes requests for advice/information.

98 A single incoming request may seek several heads of assistance. A partially acceded request is a request which contains more than one head of assistance, and some of which are acceded to.

99 Requests are deemed lapsed when there is inactivity from the requesting state for at least nine months.

100 Includes 5 cases where the offences are not specified.

101 Includes 5 cases where the offences are not specified.

102 Includes 5 cases where the offences are not specified.

103 Includes 12 cases where the offences are not specified.

104 The Average Turnaround Times indicated here are the averages of all the turnaround times for completed requests (*i.e.* Acceded, Rejected and Partially Acceded Requests). Pending, Lapsed and Withdrawn Requests are excluded from this figure. Given the complexity of Requests, such as whether the Request is complete or complies with our MACMA provisions (*e.g.* undertakings/assurances), whether the information supplied is sufficient for our action, whether further evidence/information / clarification are needed, whether Court action is required etc., it is felt that this method of determining the Average Turnaround Times would give the fairest estimate possible.

105 These cases are classified differently from other MACMA requests as they deal with terrorist related offences and may have been referred to AGC via other government agencies.

time frames before any assistance was forthcoming. Moreover, Singapore was not considered a favourable MLAT-partner because it insisted on a list-based approach to dual criminality. Thus, according to at least one country, one of its largest domestic banks has a branch in Singapore, and that country is unable to obtain necessary information for its own investigations. Thus, the lack of adequate provisions for mutual legal assistance in providing financial information has, at least in part, in the past provided a *de facto* bank secrecy situation. Despite the reciprocal provisions of the 2006 version of MACMA, there remains a perception on the part of a number of countries that the absence of a bilateral treaty may hamper the receipt of bank records from Singapore. However, it should be noted that no FATF/FSRB members raised any substantial concern about their experience with Singapore in relation to mutual legal assistance, subsequent to the April 2006 amendments. To the contrary, those countries with experience with Singapore since April 2006 indicated that their experiences had improved.

Additional elements

871. Statistics on formal requests for assistance made or received by law enforcement authorities are also kept.

6.3.2 Recommendations and Comments

872. The 2006 MACMA legislation appears to have addressed some major deficiencies in mutual legal assistance encountered in foreign requests to Singapore for assistance. However, there has not been sufficient time to show whether the provisions are working fully effectively. The Singapore authorities have highlighted various steps taken to publicise the new laws. For example, the amendments to MACMA were published in the Gazette and announced publicly in Parliament. MACMA is also reproduced on the AGC website, with a clear explanation of the mutual assistance regime, the requirement for a reciprocity undertaking in lieu of a mutual legal assistance treaty, and soft copies of the forms needed to make various mutual legal assistance requests (http://www.agc.gov.sg/criminal/mutual_legal_asst.htm). However, Singapore should consider taking the initiative in making positive steps to inform foreign governments, particularly its neighbours in the Pacific Rim and Southeast Asia regions, that it may now provide a wide spectrum of mutual assistance, and the manner in which that assistance may be sought.

873. As indicated, there are still concerns that production orders for bank information is more difficult to obtain through mutual assistance requests than perhaps other types of information, although according to Singapore, such concerns are unfounded. In addition, Singapore should change its definition of "instrumentality order" to include instrumentalities of all "serious offences" under the CDSA, and include instrumentalities "intended for use" in FT, ML, and predicate offences.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	**LC**	• Singapore may not be able to freeze, seize and confiscate based on foreign orders against instrumentalities of crime, and their equivalent amounts, or instrumentalities "intended for use" in some cases of FT, ML, and predicate offences. • It is too soon to assess the effectiveness of the current MACMA (recently amended) and Singapore's responses to foreign countries seeking to become "prescribed" for case-by-case assistance. However, there remains one concern which existed under the previous regime: the requirement for more cumbersome procedures to obtain financial institution information than other types of information.
R.37	**C**	• This Recommendation is fully observed.
R.38	**LC**	• Singapore may not be able to freeze, seize and confiscate based on foreign orders against instrumentalities of crime, and their equivalent amounts, or instrumentalities "intended for use" in some cases of FT, ML, and predicate offences.
SR.V	**LC**	• The deficiencies identified in relation to R.36, also impact the rating for SR.V.

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
		• The deficiencies identified in relation to R.38, also impact the rating for SR.V. • There is only limited authority for Singapore to freeze, seize and confiscate instrumentalities of terrorism and terrorist financing at a foreign government's request, under Singapore's domestic provisions of TSOFA.

6.4 Extradition (R.39, 37, & SR.V)

6.4.1 Description and Analysis

Recommendation 39 and Special Recommendation V

874. ML is an extraditable offence as it is listed in the First Schedule to the Extradition Act. (#26 of the Schedule). Thus, extradition of individuals charged with a ML offence to and from Malaysia and 39 declared Commonwealth countries and territories is possible in the absence of a separate extradition treaty: see Sections 18 to 39 of the Extradition Act, and the Extradition (Commonwealth Countries) (Consolidation) Declaration.

875. Extradition to non-Commonwealth countries, other than parties to the FT Convention for terrorism financing offences, is possible if there is a bilateral extradition treaty with the requesting country. Singapore currently has bilateral extradition treaties with United States, Germany and Hong Kong Special Administrative Region. Singapore has recently signed a bilateral extradition treaty with Indonesia and it is pending ratification by both countries.

876. Likewise, FT offences are deemed extraditable crimes under the Extradition Act by virtue of section 33(1) of the TSOFA. This applies to Malaysia, the three treaty countries, Commonwealth countries, and all other countries that have ratified the FT Convention. Terrorist acts would ordinarily be covered by the general list of offences in the First Schedule to the Extradition Act (*e.g.* murder, culpable homicide, maliciously or wilfully wounding or inflicting grievous bodily harm).

877. Using the FT Convention as a mechanism for extradition presents a possible problem in that the FT offences covered in the FT Convention only cover terrorist acts, whereas the FATF Recommendations, as well Singapore domestic law, also covers the collection and provision of funds to be used by terrorist organisations or individual terrorists. Therefore there is a concern that extradition could not be provided for these latter offences. However, section 33(2) and (3) of TSOFA provide that a Ministerial notification in the Gazette under section 4 of the Extradition Act may be made applying the Extradition Act as if there were an extradition treaty between Singapore and that country (s.33(2) TSOFA). Thus, section 33 of TSOFA could technically permit Singapore to extradite persons for all of Singapore's FT offences (which are largely compliant with the FATF criteria). This would include financing of terrorist acts, as well as the collection or provision of funds to be used by terrorist organizations or individual terrorists (s.3-6 TSOFA). However, it is unclear if how many countries, if any, have been designated in the manner, and therefore the effectiveness of these provisions has not been demonstrated.

878. Singapore can extradite its own nationals. The Extradition Act does not draw any distinction based on nationality.

879. The Extradition Act contains prescribed timelines for processing extradition requests which apply to all proceedings, including those relating to ML, FT and predicate offences (s.11, 12, 13, 25, 27, 28 Extradition Act). There are therefore legal safeguards to ensure that extradition requests are handled without undue delay.

Additional elements

880. There are expedited extradition arrangements between Singapore and Malaysia under sections 32 to 39 of the Extradition Act. Warrants of arrest and summonses from Brunei Darussalam and Malaysia may also be served in Singapore pursuant to the simplified procedure (s.55 CPC).

Recommendation 37 (dual criminality relating to extradition)

881. Dual criminality is a requirement for extradition. The foreign offence in question must correspond to an extraditable offence listed in the First Schedule of the Extradition Act. Singapore does not insist on a strict elements test, and uses a conduct-based approach instead. This is evident from the way "extradition crime" is defined in section 2(1) of the Extradition Act. It refers to an offence against the law of, or of a part of, a foreign State and the act or omission constituting the offence or the equivalent act or omission would, if it took place in or within the jurisdiction of Singapore, constitute an offence against the law in force in Singapore that is described in the First Schedule of the Extradition Act. Examination is therefore made of the underlying conduct as a whole, and not based on the label or elements of the offence in the foreign State. Technical differences in the manner in which another country categorises or denominates the offence accordingly does not pose an impediment to the provision of extradition.

882. A 10 September 2007 amendment to the Extradition Act provides for extradition in instances of abetment and conspiracy to commit a "serious crime" as defined by the Palermo Convention.

Statistics and effectiveness

883. The following chart sets out the number of extradition requests received by Singapore from 2004 to July 2007.

Incoming Extradition Requests (as of July 2007)

	2004	2005	2006	2007 (up to July)
Incoming requests	5	6	7	5
Concluded requests	2	1		
Processed requests[106]	1	3	5	2
Pending requests	1	1		2
Rejected requests	1	1	2	1
Nature of offence –ML/TF	0	0	0	0
Fraud/Cheating/DRSP	4	3	2	1

884. Out of 23 extradition requests since 2004, only five were outright rejected. Foreign countries did not voice the same concerns about extradition requests to Singapore as they did about MLA requests for bank information

6.4.2 Recommendations and Comments

885. Outside of Commonwealth countries, Malaysia, and three treaty countries, extradition cannot be provided for FT offences not covered in the CFT Convention (provision/collection of funds for a terrorist country or individual terrorist), unless they have been designated in the Gazette. The effectiveness of this process has not been demonstrated. Singapore should consider streamlining its procedures for extraditing for FT offences not covered in the CFT Convention to ensure that Singapore can rapidly respond to such requests.

[106] *E.g.* -fugitive not within jurisdiction; bare requests; not an extraditable offence or a criminal matter; requesting person is a private party.

6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	**C**	• This Recommendation is fully observed.
R.37	**C**	• This Recommendation is fully observed.
SR.V	**LC**	• Outside of Commonwealth countries, Malaysia, and three treaty countries, extradition cannot be provided for FT offences not covered in the FT Convention (provision/collection of funds for a terrorist country or individual terrorist), unless they have been designated in the Gazette. The effectiveness of these provisions has not been demonstrated.

6.5 Other Forms of International Co-operation (R.40, SR.V & R.32)

6.5.1 Description and Analysis

Recommendation 40 and SR.V (Other forms of international cooperation)

886. As far as the sharing of financial information is concerned, the legal framework in Singapore stipulates that such assistance comes under the Mutual Assistance in Criminal Matters Act (MACMA). However, it is possible for assistance to be provided under MACMA even if the requesting country does not have a Mutual Legal Assistance Treaty with Singapore, subject to the discretion of the Attorney-General (which is the designated competent authority in such matters) and on a case-by-case basis.

887. The provisions described below relating to the ability of the FIU, law enforcement and supervisory authorities to provide other types of international co-operation apply equally to matters involving money laundering and terrorist financing.

FIU to FIU Exchange of Information

888. STRO can provide a wide range of assistance which includes obtaining public records (*e.g.* company registration information), conducting site visits, locating witnesses, recording voluntary statements, criminal record information (where applicable), etc. STRO is also allowed to provide STR information to a foreign FIU if the conditions of section 41, CDSA are fulfilled, including an undertaking that the STR information will not be used as evidence in any proceedings. There are generally clear and efficient processes in place for the execution of FIU to FIU requests in a timely and rapid manner.

Gateways for assistance

889. Generally, the STRO co-operates with its foreign counterparts through the mechanism of entering into an MOU. As at 14 November 2007, STRO has concluded 11 MOUs with its counterparts FIU. This is an increase from the 3 MOU since STRO was assessed in 2003 pursuant to the FSAP. The 11 jurisdictions are Australia, Belgium, Brazil, Canada, Greece, Hong Kong, Italy, Japan, Mexico, United Kingdom and United States.

Jurisdictions	Date MOU concluded
Belgium	7 September 2001
Australia	3 September 2002
Japan	2 July 2004 (re-sign in 27 June 2007)
United States of America	7 September 2004
Canada	28 June 2005
Brazil	29 June 2005
Greece	29 June 2005
Hong Kong	16 May 2006
Italy	21 July 2006
Mexico	11 October 2006
United Kingdom	9 October 2007

890. A number of other MOUs are still under negotiation. These include Switzerland, Ireland, Russia, Argentina, Portugal, South Korea, Israel, People's Republic of China, and Turkey. In addition, Singapore has previously approached the following jurisdictions and is awaiting a favourable response from them: France, Germany, Netherlands, New Zealand, Denmark, Finland, Austria, Iceland, Luxembourg, Norway, South Africa, Spain, and Sweden.

891. Upon joining the Egmont Group of FIUs in July 2002, STRO institutionalised a policy whereby STRO would render all members of the Egmont Group of FIUs the types of assistance that STRO would normally offer police or law enforcement units. This is regardless of whether the foreign FIU is a police unit or not. The effect of this policy is that a wider range of assistance may be provided to the foreign FIU even without a Memorandum of Understanding.

892. Moreover, as a member of the Egmont group of FIUs, STRO is also able to exchange information through the Egmont network. The information shared through the Egmont channel includes known criminal records, business records and other relevant information requested (subject to any restriction imposed law). As an enforcement style FIU, STRO is also able to have access to other forms of cooperation normally available to enforcement agencies (*e.g.* Interpol).

893. STRO is able to exchange information spontaneously with its MOU partners and reports that it has in fact done so on a regular basis. This is explicitly provided for under section 41 of the CDSA, which stipulates that there is a reciprocal arrangement to share information and that STRO is satisfied that the corresponding authority will maintain confidentiality and will not use the information in criminal proceedings. STRO states that it has received favourable comments from its MOU partners on the spontaneous exchange of information that it has provided. In addition, STRO has participated in the spontaneous exchange of information vis-à-vis the Egmont Group of FIUs as well as the Interpol channels in STRO's capacity as an enforcement style FIU.

894. STRO is able to exchange information with its foreign counterparts in response to a request for information. In such cases, the information exchange must be performed in accordance with the terms of the MOU (as well as the best practices of the Egmont Group of FIUs). As well, the foreign FIU is required to provide some brief facts about the matter they are looking into, and the intended use of the information sought for.

895. As STRO is a 'police' type FIU, the assessment team queried, from within the amended legislation, the use of the terms 'corresponding authority' and that the foreign authority is required to be 'investigating' drug trafficking or serious offence. The Singapore authorities stated that 'corresponding authority' included non-police type FIUs and that since the term 'investigating was not defined in the legislation they would use the common usage definition which included 'inquiry'. In other words they saw no problem in the STRO being able to cooperate with a foreign non police FIU that was inquiring about one of these types of matters.

Inquiries on behalf of counterparts

896. An STRO officer is able to search STRO's database to facilitate the exchange of financial intelligence. This must be conducted in accordance with Singapore's domestic framework. In addition, STRO, as an enforcement-style FIU is also able to access the various enforcement databases available to the SPF as well as public databases and is able to share the information residing in these databases (s.41 CDSA).

897. The exchange of information is subject to Singapore's national legislation and strict rules of confidentiality. Section 41(1) of the CDSA allows STRO to communicate STR information to a foreign FIU provided that there is an arrangement (*e.g.* an MOU) for such exchange on the basis of reciprocity and confidentiality. Additionally, the provision of information by the STRO is limited by the stated purpose of the requesting agency and cannot be disseminated without STRO's prior consent. The information provided by the STRO is only for intelligence purposes and should not be used as

evidence in court. Requests for cooperation are not rejected on the sole ground that they are considered to involve fiscal matters. STRO is able to share information which would include those subject to secrecy laws on financial institutions and DNFBPs provided that:

(a) There is a legal basis (*e.g.* MOU, MACMA Requests) to share.

(b) There is the commission of an offence or foreign serious offence under CDSA.

(c) It is not subject to legal privilege.

898. As such, laws that impose secrecy or confidentiality requirements are not grounds for refusal of cooperation.

Controls and safeguards

899. Requests for assistance received through the Egmont channels are frequently sent from one FIU to another FIU. In accordance with Egmont principles, the request for assistance is only to be disseminated to the requesting party. It is incumbent on the requesting FIU to state the purpose for which the information is requested and permission has to be sought if the information requested is to be disseminated to another agency. STRO has adhered to this Egmont principle strictly and all information received by STRO or requested from STRO is kept confidential and is not disseminated to officers which are not part of STRO unless prior consent has been sought from the requesting authority. STRO would also not reveal any information obtained from the requesting authority to a third party unless such consent was given previously. Additionally, all information received by STRO is treated as the same level as any information that is obtained locally and is subject to protection under the Official Secrets Act and section 56(1) CDSA, as the case may be.

Statistics and effectiveness

900. STRO has been working on increasing its level of spontaneous exchange of information. STRO indicated that it has also received positive feedback on the information provided and will continue to provide useful intelligence to its counterparts. Please see the table below for consolidated statistics.

Table - Requests for Assistance made/received by STRO

	2004	**2005**	**2006**	**2007 (as at 14 Nov.)**
Requests for Assistance Received by STRO	102	81	69	76
Request for Assistance Received from FIU Partners	47	59	54	59
Requests received from MOU partners	5	15	15	7
Responses Provided for Request for Assistance	102	81	69	76
Requests for Assistance Made by STRO (to Foreign Authorities)	66	66	43	58
Spontaneous Exchange of Information Provided	68	53	55	71

901. STRO has also made a number of requests for assistance, whether for itself or in order to assist a local enforcement agency in its investigations, through its FIU counterparts. The information obtained through these requests for assistance has been helpful in developing STRO's intelligence and had assisted in a number of investigations, including money laundering investigations. The following chart sets out the number of foreign requests that STRO has granted or partially granted (acceded) and refused (not acceded).

	2004	2005	2006	2007 (As at 14 Nov.)
Requests Acceded	62	53	47	55
Requests Partially Acceded	28	19	18	14
Requests Not Acceded	12	9	4	2
Requests pending assessment	**0**	**0**	**0**	**5**
TOTAL	**102**	**81**	**69**	**76**

902. Of the 328 requests for assistance that STRO received from foreign authorities, about 1/3 were refused or only partially granted. Singapore authorities indicate that all requests for assistance that fall within the functions of STRO and are consistent with its legal framework are accepted by STRO. In most, if not all, cases of requests not being acceded (or partially acceded) by STRO, the requesting party has asked for assistance that is not within STRO's power to render. For example, STRO may be asked at first instance to provide assistance that would ordinarily come under the framework of a Mutual Legal Assistance Treaty or if the nature of the incoming request from a non-MOU partner includes a request for financial information from a financial institution. For such cases, STRO would advise the requesting FIU to submit the request via the proper channel and provide guidance on how this could be done. STRO will also be able to provide information on other information requested such as company details on directorships and shareholdings as well as information on criminal investigations and previous criminal convictions. In such cases, the request would be partially acceded to. If a similar incoming request comes from a MOU partner, Singapore is able to share all information contained in the STRO database. Such information would include relevant financial information, details of Suspicious Transaction Reports and other information obtained in the course of the analysis and investigation of the STRs. In such cases, the request would be fully acceded to.

903. The time taken to respond to incoming requests depends on the urgency of the request. For urgent request, responses are usually given immediately or within 1 or 2 days. For a normal request, time taken to respond can vary between 1 to 4 weeks depending on the amount of information required and provided.

Police to Police Exchange of Information

904. The Singapore Police Force is active in The International Criminal Police Organisation (Interpol)[107] (as well as the ASEANAPOL) and utilises mechanisms through that body to exchange information with its foreign counterparts. A specialised branch (NCB Singapore) has been established in the Criminal Investigation Department to ensure that all exchange of information through the Interpol channel is handled expeditiously and effectively. The key conduit through which SPF exchanges information with its foreign counterparts is the I-24/7 system to communicate with Interpol's 186 member states on matters related to criminal Investigations, training and conferences. All foreign requests on criminal investigations that are sent to NCB Singapore (International Affairs Branch) are addressed in accordance to Singapore domestic law and police procedures, as well as in accordance to treaties, MOUs or agreements signed by Singapore with foreign countries (if applicable). If the requests for assistance are under the purview of other enforcement agencies, they are channelled to the relevant enforcement agencies (*e.g.* FIB and PCU) in Singapore for follow-up actions.

905. The SPF has also concluded MOUs with some of its strategic partners to enhance bilateral exchanges as well as joint co-operation in various fields. In particular, SPF has concluded MOU on "Combating Transnational Crime and Developing Police Co-operation" with counterparts in Australia, Brunei and more recently South Korea.

[107] Singapore's Commissioner of Police was elected the Vice-President of the Executive Committee from 2006 to 2009. Singapore also hosted the ASEANAPOL Conference (2 to 7 June 2007).

906. Singapore authorities indicated that they regularly shared information informally with many of their counterparts including relevant authorities in Malaysia, Australia and the United States. This information consisted of information that was accessible through public databases such as land ownership records, and police records such as criminal history, police intelligence and drivers licences etc. However it was highlighted that certain information that had protection under legislation, such as financial institution records, required formal requests and could not be supplied under informal requests.

907. The Singapore Police are able to co-operate through normal police to police information exchange channels. Inquiries can be made through counterparts and through Interpol. The Criminal Police have the authority to conduct investigations on behalf of foreign counterparts and joint investigations are possible. For example the CNB cooperates actively with foreign law enforcement agencies on a bilateral basis. Such cooperation usually entails the exchanges of information/intelligence relating to drug trafficking and drug related money laundering offences. CNB also liaises with the International Criminal Police (Interpol) and the Regional Intelligence Liaison Office (RILO) of the World Customs Organisation. CNB has also rendered international intelligence cooperation to various foreign agencies. From 2004 to 2006, CNB has rendered assistance to foreign agencies such as US Drug Enforcement Administration and the Australian Federal Police.

908. As part of the Singapore Police the STRO is able to exchange information spontaneously with its MOU partners and reports that it has in fact done so on a regular basis. This is explicitly provided for under section 41 CDSA: STRO's ability to exchange information is conducted in accordance with Singapore's domestic legislation and is conducted with regard to money laundering, terrorism financing as well as the underlying predicate offence and if the information resides in STRO's database.

Inquiries on behalf of counterparts

909. Law enforcement authorities can assist the relevant authority of a foreign country to conduct informal inquiries by recording voluntary statements from witnesses subject to their consent.

910. Law enforcement authorities including the SPF, CNB, CAD and CPIB are authorised to conduct investigations on behalf of foreign counterparts and officers from these authorities are "authorised officers" for the purposes of MACMA. A "criminal matter" includes "criminal investigation", which includes an investigation into a Singapore offence or a foreign offence, as the case may be (s.2(1) MACMA). The types of investigations they can conduct include locating and identifying a person pursuant to a request by the appropriate authority of a foreign country (s.37 MACMA), assisting in the process of taking evidence for criminal proceedings (s.21 MACMA) assisting in the process of obtaining production order in respect of a thing (s.22 MACMA), assisting in obtaining search warrant and conducting search of premises and seizure of things specified in the search warrant, including photographing or making a copy of the things seized (s.33 to 35, MACMA).

911. The scope and extent of information exchange, as well as any relevant condition to be attached, usually accord with accepted international standards and practices. Requests for co-operation are not rejected on the sole ground that it is considered to involve fiscal matters. Singapore does not refuse cooperation on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBPs; however, they do require official requests, complying with legislative conditions, to conduct these enquiries.

912. Like STRO officers, the law enforcement authorities are required to treat all information received as the same level as any information that is obtained locally and is subject to protection under the Official Secrets Act and section 56(1) CDSA, as the case may be.

Customs/ Immigration to Customs Exchange of Information

913. Although the ICA did not have any MOUs with its counterparts, it was very active in developing international informal networks with officers from other jurisdictions, in the form of foreign training exchanges, conferences and workshops.

914. The ICA uses these networks and other informally gained networks to constructively communicate information promptly between counterparts. ICA indicated that it had not encountered any problems in communicating with other counterparts and did so on regular occasions. Intelligence reports for other jurisdictions are also regularly disseminated through the Intelligence Division. The Singaporean authorities also indicated that, in instances where a more formal system of co-operation is required, they may use the existing system that is used by other security agencies under the Ministry of Home Affairs (*e.g.* SPF or CNB).

915. The ICA's experience in dealing with informal requests by foreign agencies usually entails the exchange of intelligence relating to Customs or Immigration type offences. ICA reports that information of this type is regularly exchange with their counterparts.

916. As the ICA refers all non-immigration/customs offences to other investigating authorities. Exchanges of information relating to money laundering and underlying predicate offences are handled by agencies such as CAD. The ICA generates intelligence reports on such matters and can disseminate such information spontaneously.

Inquiries on behalf of counterparts

917. As the ICA refers all non-immigration/customs offences to other investigating authorities inquiries on behalf of foreign authorities is also conducted by other agencies such as the CAD. The scope and extent of information exchange, as well as any relevant condition to be attached, conforms with accepted international standards and practices. Requests for cooperation are not rejected on the sole ground that they are considered to involve fiscal matters. Like any of the other Home Team agencies the ICA are required to treat all information received as the same level as any information that is obtained locally and is subject to protection under the Official Secrets Act and section 89 Customs Act.

Additional elements

918. Other requests for assistance relating to ML/FT are handled by STRO's sister units (*i.e.* FIB and PCU). The number of such request handled by FIB and PCU since 2005 are:

Request for Assistance Received by FID

	2004	2005	2006	2007 (14 Nov 2007)
Requests for Assistance Received by FIB and PCU relating to ML / TF	0	5	34	45

Supervisor to supervisor exchange of information (MAS)

919. There are provisions in section 45(1) of the Banking Act, Part IIIA, Insurance Act, Part X, Securities and Futures Act and Part VII, Financial Advisors Act for, and a practice of information sharing between, MAS and its counterpart financial regulators in other jurisdictions. While MOUs are not required for this purpose, MAS has nonetheless established a system of information sharing and mutual assistance that sets out the processes and procedures to facilitate such cooperation. Essentially, these MOUs provide an agreed arrangement for supervisory co-operation between MAS and foreign financial regulators. These MOUs are consistent with internationally agreed principles that guide cross-border supervisory co-operation between financial regulators. This helps to strengthen the

supervision of cross-border operations of financial institutions under both authorities' purview. Currently, MAS has MOUs with the following:

1. The China Banking Regulatory Commission
2. The Bank of Thailand
3. The Financial Supervisory Commission of the Republic of Korea
4. The Insurance Authority of the Hong Kong Special Administrative Region of the People's Republic of China on regulatory cooperation
5. China Insurance Regulatory Commission
6. State Securities Commission of Vietnam
7. The Securities and Exchange Commission in Taipei on the Exchange of Information Concerning Commodity Futures and Options
8. The China Securities Regulatory Commission
9. Republique Francaise - Commission Des Operations De Bourse
10. United States Securities & Exchange Commission Commodity Futures Trading Commission
11. Australian Securities and Investments Commission
12. Federal Republic of Germany - Bundesaufsichtsamt Fur Den Wertpapierhandel
13. Federative Republic of Brazil - Comissao De Valores Mobiliarios
14. Quebec, Canada - Commission Des Valeurs Mobilieres De Quebec
15. The Financial Services Board of the Republic of South Africa
16. The Financial Services Agency of Japan
17. The Securities & Exchange Board of India - Govt of India
18. Commissione Nazionale Per Le Societa' e la Borsa Italy [CONSOB]
19. The Emirates Securities and Commodities Authority, Declaration of Intent on a MoU on Bilateral Cooperation Between MAS and the Emirates Securities & Commodities Authority
20. Commission de Surveillance du Secteur Financier
21. United Kingdom Financial Services Authority
22. State Bank of Vietnam
23. Swiss Federal Banking Commission

920. MAS has also exchanged information with regulators without formal MOUs. These include the Financial Services Commission of Mauritius, Banca D'Italia, and the French Banking Commission. Singapore has also signed the 1996 IOSCO exchange and clearing house MOU of Boca Raton, Florida.

921. Singapore laws allow a home country supervisor to conduct on-site examinations of the Singapore branch of a bank under its supervision to verify for compliance with home country KYC policies and procedures of their branch in Singapore. The Head Office internal auditors of the bank are also allowed to conduct on-site examinations. In accordance with the Supervision of Cross-Border Banking Report (BIS, 1996), alternatives are available as Singapore allows the banks to engage local auditors to sample individual customer accounts, or MAS can perform the inspections and report the findings to the parent supervisors.

922. Other regulatory Acts, such as the Insurance Act, the Securities and Futures Act and the Financial Advisors Act provide for MAS to give assistance to foreign regulatory authorities or other authorities under certain conditions.

923. MAS provides financial information to foreign regulators to assist them in their investigations, which pertain mostly to securities and futures transactions. On average, MAS takes between one to four weeks to respond to such requests depending on the nature of the requests. As far as it considers it necessary and appropriate, MAS provides spontaneously inspection reports on foreign financial

institutions to the home country supervisors. It also fosters a proactive dialogue and gives feedback on issues of prudential concern to home country regulators. Other ways of exchanging supervisory information practiced by Singapore include bilateral meetings with neighbouring and other major regulators, and answering a few hundred requests from foreign regulators seeking information on individuals and companies (fit and proper checks) within, on average, 7.5 days.

924. MAS is able to exchange information both spontaneously and upon request and relating to ML, FT and predicate offences.

Inquiries on behalf of counterparts

925. Singapore does not refuse co-operation on the basis of secrecy or confidentiality requirements. The Securities and Futures Act and the Insurance Act provide that MAS, in relation to a request by a regulatory authority of a foreign country for assistance, may order any person to share directly with the regulatory authority or indirectly through the intermediation of MAS information and materials, notwithstanding any obligation as to secrecy or other restrictions upon the disclosure of information by law, rule of law, contract or rules of professional conduct. MAS also has the authority to inspect or make at any time an investigation of any bank in Singapore (s.43 Banking Act). Section 44A of the Banking Act also provides that customer information that is obtained by MAS from a bank incorporated outside Singapore or a foreign-owned bank incorporated in Singapore during an inspection or an investigation, may be disclosed by MAS to the parent supervisory authority of the bank where this is required by the parent supervisory authority for the purpose of carrying out its supervisory functions. This information may be shared when:

- The customer information does not consist of deposit information.
- The customer information is required by the parent supervisory authority for the sole purpose of carrying out its supervisory functions.
- The parent supervisory authority is prohibited by laws applicable to the parent supervisory authority from disclosing the customer information obtained by it to any other person or has given the MAS such written undertaking, as to the confidentiality of the information obtained.

926. Where there is suspicion of criminal activity, MAS, in line with Basel Core Principles, is able to share customer information related to suspected or actual criminal activity where information is used for supervisory purposes. Although not explicitly mentioned, it may be assumed that other, less delicate non-public information may be shared as well under the same conditions, including confirmation that the information is needed for the sole purpose of carrying out supervision, and confirmation of confidentiality. Also, as a foreign supervisory authority can, with the written approval of MAS appoint another body to conduct an inspection of its Singapore branch (s.45(4) Banking Act), MAS can be asked to perform the inspection itself and report the findings to the parent supervisor as part of supervisory co-operation.

927. For the securities, insurance and financial advisors sectors, MAS has the authority to obtain and share with foreign regulators public and non-public information in order to assist the foreign regulator to carry out supervision, investigation and enforcement.

928. While MAS must observe confidentiality, it is empowered by Part X of the SFA (in relation to the securities sector) and Part IIIA of the IA (in relation to the insurance sector) to exchange information with foreign regulators if it is satisfied that the information requested is necessary for the foreign regulator's purpose as specified in its request. Other preconditions for assistance include the gravity of the offence and that rendering assistance is not contrary to public interest. A similar power is also provided to MAS to exchange information with foreign regulators on Financial Advisors (s.78 and 80, Part VII FAA). The scope and extent of information exchange, as well as any relevant condition to be attached, usually accord with accepted international standards and practices.

929. Requests for cooperation are not rejected on the sole ground that they are considered to involve fiscal matters. Singapore does not refuse cooperation on the basis of secrecy or confidentiality requirements on financial institutions. The Banking Act provides specifically that customer information (which is normally covered by the banking secrecy) that is obtained by MAS from a bank incorporated outside Singapore during an inspection or an investigation may be disclosed by MAS to the parent supervisory authority of the bank where the customer information does not consist of deposit information, is required by the parent supervisory authority for the sole purpose of carrying out its supervisory functions and the parent supervisory authority is not permitted by law or by an agreement with MAS to disclosing the customer information obtained to any other person (s.44A(4), Banking Act).

930. Other Acts provide that MAS in relation to a request by a regulatory authority of a foreign country for assistance may order any person to share directly with the regulatory authority or indirectly through the intermediation of MAS information and materials notwithstanding any obligation as to secrecy or other restrictions upon the disclosure of information by law, rule of law, contract or rules of professional conduct. An exception is foreseen only for advocates and solicitors as far as their privileged communications are concerned (s.49D, Insurance Act; s.172, Securities and Futures Act; s.80, Financial Advisory Act).

931. MAS must treat all information that it receives at the same level as any information that is obtained locally and is subject to protection under the Official Secrets Act. In addition, the following legislation also imposes statutory confidentiality obligations on MAS officers. Section 14 of the MAS Act requires employees to maintain confidentiality on information obtained while exercising their functions, except where lawfully required to divulge that information. Section 3 of the Statutory Bodies of Government Companies Protection of Secrecy Act has similar provisions.

Statistics and effectiveness

932. The following chart sets out a breakdown of the requests that the MAS has received from foreign counterparts. All of these requests have related to predicate offences, not ML. However, at the time of the on-site visit there was one request pending that was received in September 2007 which may have related to ML – although this – was not certain and MAS was still corresponding with the requesting regulator on the matter. [108]

Requests for assistance for predicate offences

	2004	2005	2006	2007 (as at 14 Nov.–)
Received by MAS				
Number of requests received	7	4	12	10
Number of requests granted	6	4	11	8
Number of requests refused	1	-	-	-
Number of requests referred to CAD	-	-	1	1
Number of requests pending	-	-	-	1
Made by MAS				
Number of requests made	3	4	5	2
Number of requests granted	3	4	4	2
Number of requests refused	-	-	1	-

[108] Subsequently, based on the information contained in the request and other information received, MAS took regulatory action on Dec 2007 against the financial institution involved and referred the matter to CAD for investigation into possible money-laundering offences.

933. MAS provides a wide range of international cooperation to its counterparts in a timely manner. Particular features are its pro-active stands in sharing inspection results spontaneously with its foreign counterparts in order to have compliance weaknesses addressed and to guarantee quality improvements. Singapore makes efforts to have processes and procedures in place to facilitate the international cooperation by voluntarily concluding MOUs with foreign supervisory authorities. The FATF has received no negative comments with regard to MAS' international cooperation in response to FATF's request for international co-operation information to the delegations in view of the mutual evaluation of Singapore.

Additional elements

934. STRO, apart from exchanging information with its counterpart FIU has been actively engaging and pursuing other non-counterpart agencies, such as foreign police units. Whenever possible, STRO will seek to assist these other agencies within the confines of Singapore's domestic legislation. STRO is able to obtain information from other agencies and share it with its foreign counterparts so long as consent is obtained from the agency and there is no legal restriction on the sharing of such information. Being a law enforcement style FIU, STRO has the additional capability to share information relating to the police with its foreign counterparts.

6.5.2 Recommendations and Comments

935. Singapore is fully compliant with this Recommendation.

6.5.3 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	**C**	• This Recommendation is fully observed.
SR.V	**LC**	• This Recommendation is fully observed with respect to R.40.

7. OTHER ISSUES

7.1 Resources and Statistics

936. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report *i.e.* all of section 2, parts of sections 3 and 4, and in section 6. There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report contains the boxes showing the rating and the factors underlying the rating.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
R.30	**C**	• This Recommendation is fully observed.
R.32	**LC**	• The statistics relating to the number of cases and amounts of property frozen, seized and confiscated do not specifically distinguish between cases in which there is a close relation between the domestic predicate offences and the money laundering investigations. • Singapore does not maintain statistics concerning the volume of international wire transfers.

7.2 Other Relevant AML/CFT Measures or Issues

937. There are no further issues to be discussed in this section.

7.3 General framework for AML/CFT system (see also section 1.1)

938. There are no further issues to be discussed in this section.

TABLES

TABLE 1: RATINGS OF COMPLIANCE WITH FATF RECOMMENDATIONS

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC), or could, in exceptional cases, be marked as not applicable (na).

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
1. ML offence	PC	• Effectiveness: The money laundering offence is not effectively implemented as is shown by: the low number of ML prosecutions and convictions, given the size of Singapore's financial sector and the level of ML risk. Also there is a focus on pursuing domestic predicate offence cases, with ML as an ancillary crime, rather than ML as a separate offence, which results in few third party ML cases being pursued and insufficient attention being paid to ML involving the proceeds of foreign predicate offences. • An additional "purposive" mens rea requirement in CDSA Sec. 46(2) and 47(2) in relation to the offence of "concealment or disguise", and a missing alternative purpose element in relation to the offence of "conversion or transfer" are inconsistent with the Conventions and may hamper the government's ability to prosecute third-party ML cases under those sections.
2. ML offence – mental element and corporate liability	LC	• The money laundering offence is not effectively implemented as is shown by the low number of overall ML prosecutions and convictions (given the size of Singapore's financial sector and the level of ML risk), the low range of sentences being applied, and the focus on pursuing domestic predicate offences rather than ML which results in few third-party ML cases being pursued and insufficient attention being paid to ML involving the proceeds of foreign predicate offences. No prosecutions have been brought against any legal persons.
3. Confiscation and provisional measures	LC	• The restraint provisions do not extend to property of corresponding value, and it is unclear whether restraint provisions extend to all instrumentalities and intended instrumentalities of crime. • Effectiveness: Given the risk of money being laundered in Singapore (particularly the proceeds of foreign predicate offences), the amount of money being frozen and seized seems low. The procedure for obtaining bank records (by High Court order through application by the AGC) is cumbersome compared to the procedure by which the police may simply seek a court order directly (i.e., without going through the AG) from either the High Court or District Court to obtain all other information – without any apparent reason to differentiate between the two types of evidence.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	C	• This Recommendation is fully observed.
5. Customer due diligence	LC	• Certain requirements (when CDD takes place, required CDD measures, beneficial ownership, on-going due diligence) are contained in the Notices, which while they create legally enforceable obligations with criminal sanctions for non-compliance, are not in law or regulation as defined by the FATF.

		• It is not specified that simplified CDD provisions are not allowed whenever there is suspicion of ML/TF. • Non-bank FIs do not necessarily conduct sufficient risk assessments of new customers with a view to determining whether they are high risk customers to whom enhanced CDD measures should be applied. • Scope issues—commodity futures brokers will only be covered in 2008, and the implementation of CDD measures to moneylenders is too new to be assessed.
6. Politically exposed persons	LC	• Scope issues—commodity futures brokers will only be covered in 2008.
7. Correspondent banking	C	• This Recommendation is fully observed.
8. New technologies & non face-to-face business	LC	• Scope issues–commodity futures brokers will only be covered in 2008 by general requirements concerning non-face-to-face business, and the implementation of relevant measures to moneylenders is too new to be assessed.
9. Third parties and introducers	LC	• No requirement that FIs should immediately obtain CDD information on introduced customers. • Scope issues–commodity futures brokers will only be covered in 2008.
10. Record keeping	LC	• The requirements to maintain business correspondence are set out in other enforceable means, not law or regulation. • Commodities futures brokers will only be covered in 2008.
11. Unusual transactions	LC	• Commodities futures brokers are not yet covered. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
12. DNFBP – R.5, 6, 8-11	NC	• Real estate agents, dealers in precious metals and stones, accountants, and trust service providers (other than trust companies) and company service providers do not have any AML/CFT obligations pertaining to Recommendation 12. <u>*Lawyers:*</u> • The measures to implement Recommendation 5 suffer from the following deficiencies: - There is no specific requirement to conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data. - There is no specific requirement for lawyers to identify the beneficial owner for all customers or to determine if the customer is acting on behalf of another person. - There is no specific requirement to understand the ownership and control structure of the customer. - The requirement to understand the nature and purpose of the business relationship does not apply to all circumstances required by the FATF Recommendations. - There is no general requirement for lawyers to conduct on-going due diligence of the customer or ensure that information collected under the CDD process is kept up-to-date. - Enhanced due diligence is not generally applied to all high risk customers. - Certain specified categories of low risk customer are completely exempted from CDD requirements, rather than being made subject to simplified CDD measures. - There is no requirement to ensure that the ML risks are effectively managed when CDD cannot be completed at the start of the business relationship. - The prohibition on an account being opened or transaction performed if the required CDD information cannot be obtained is too narrow, and does not apply to all cases.

		- There is no requirement to consider making an STR if CDD cannot be satisfactorily completed. - Effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 6, there is no requirement to conduct enhanced ongoing monitoring on relationships with clients who are PEPs. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force. • The measures to implement Recommendation 9 suffer from the following deficiencies: - There is no requirement to ensure that the intermediary/third party is regulated and supervised in accordance with the FATF Recommendations, or has measures in place to comply with Recommendations 5 and 10. - There is no requirement to consider whether the intermediary/third party is located in a country that does not adequately apply the FATF Recommendations. - There is no provision that explicitly states that the ultimate responsibility for customer identification and verification remains with the lawyer who is relying on the intermediary/third party. - Effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 10, there is no requirement to maintain business correspondence, ensure that records are kept in such a manner as to permit the reconstruction of individual transaction, and ensure that all records can be made available on a timely basis. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force. • In relation to Recommendation 11, there is no express requirement that all findings relating to unusual transactions be kept for 5 years. Also, effectiveness cannot yet be assessed, as these requirements only recently came into force.
13. Suspicious transaction reporting	LC	• The scope of the predicate offences for STR reporting does not satisfy all the FATF standards. • Certain clarifications of the law (reporting to STRO, attempted transaction) are covered in “other enforceable means” but not in law or regulation.
14. Protection & no tipping-off	LC	• The scope of the tipping-off provision does not include a case where an STR is in the process of being reported to the FIU.
15. Internal controls, compliance & audit	LC	• Commodities futures brokers will only be covered in 2008. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
16. DNFBP – R.13-15 & 21	PC	• The measures to implement Recommendation 13 suffer from the following deficiencies: - The reporting obligation is not implemented effectively (lack of understanding about the reporting obligation, and low numbers of reports being filed even though the requirements have been in place for four years). - The limitations identified under Recommendation 13 with respect to the reporting obligation also affect compliance with Recommendation 16. • The limitations identified under Recommendation 14 with respect to the tipping off provision also affect compliance with Recommendation 16. • None of the DNFBP sectors (other than lawyers and part of the TCSPs, namely the trust companies) are subject to requirements relating to R.15 and 21. *Lawyers* • The measures to implement Recommendation 15 suffer from the

		following deficiencies: - There is no requirement to implement internal controls in relation to record retention, the detection of unusual and suspicious transactions or the reporting obligation. - There is no requirement to maintain an adequately resourced and independent audit function, appoint a compliance officer or establish screening procedures to ensure high standards when hiring employees. - There is no requirement to provide training that covers FT. - Effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007). • In relation to Recommendation 21, effectiveness cannot yet be assessed, as these requirements only recently came into force (in mid-August 2007). *Trust Companies* • The limitations identified under Recommendation 15 and 21 with respect to financial institutions also affect compliance with Recommendation 16.
17. Sanctions	LC	• Effective, proportionate, and dissuasive sanctions for non-compliance with AML/CFT obligations will do not yet apply for commodity futures brokers, and the effectiveness of the sanctions for money lenders has not yet been tested.
18. Shell banks	C	• This Recommendation is fully observed.
19. Other forms of reporting	C	• This Recommendation is fully observed.
20. Other NFBP & secure transaction techniques	LC	• The issuing of the SGD 10 000 note is of some concern.
21. Special attention for higher risk countries	LC	• No enforceable powers have been exercised to require financial institutions to apply stringent or additional AML/CFT counter-measures against those countries which continue not to apply or insufficiently apply the FATF Recommendations. • Commodities futures brokers will only be covered in 2008. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
22. Foreign branches & subsidiaries	LC	• Commodities futures brokers will only be covered in 2008.
23. Regulation, supervision and monitoring	LC	• Commodity futures brokers are not yet supervised for AML/CFT, and the effectiveness of the supervisory regime for money lenders has not yet been tested. • Fit and proper tests do not apply to all senior management. • The risk of unlicensed MVTs is not adequately addressed.
24. DNFBP - regulation, supervision and monitoring	NC	• No AML/CFT supervisory regime for real estate agents. • No AML/CFT supervisory regime for dealers in precious metals and stones. • No AML/CFT supervisory regime for accountants. • No AML/CFT supervisory regime for trust and company service providers (other than trust companies). • No comprehensive AML/CFT monitoring for lawyers, and the effectiveness of the existing regime cannot yet be assessed.
25. Guidelines & Feedback	LC	• No issued guidance for trust service providers (other than trust companies and lawyers) or company service providers. • Existing guidelines for real estate agents, accountants, and dealers in precious metals and stones are not comprehensive. • No general or specific feedback given to DNFBPs concerning the reporting obligation.

Institutional and other measures		
26. The FIU	LC	• STRO's analysis is overly focused on detecting and identifying predicate offences, and is not adequately focused on detecting and identifying money laundering cases. • Minor concerns about the operational independence of the STRO.
27. Law enforcement authorities	LC	• Effectiveness: low number of investigations for ML (most of which are investigations in concert with investigations of the predicate offence); little use made of STRs to investigate ML; inadequate proactive investigation of ML related to funds coming into Singapore from another jurisdiction.
28. Powers of competent authorities	C	• This Recommendation is fully observed.
29. Supervisors	LC	• There are not AML/CFT inspection and enforcement powers for commodities future brokers. • As the provisions that apply to moneylenders are very recent, it is not yet possible to assess their effectiveness.
30. Resources, integrity and training	C	• This Recommendation is fully observed.
31. National co-operation	C	• This Recommendation is fully observed.
32. Statistics	LC	• The statistics relating to the number of cases and amounts of property frozen, seized and confiscated do not specifically distinguish between cases in which there is a close relation between the domestic predicate offences and the money laundering investigations. • Singapore does not maintain statistics concerning the volume of international wire transfers.
33. Legal persons – beneficial owners	PC	• While the investigative powers are generally sound and widely used, there are limited measures in place to ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. • Information on the company registrar pertains only to legal ownership/control (as opposed to beneficial ownership), is not verified and is not necessarily reliable. • Foreign companies are not required to keep information on shareholders, nor changes to shareholdings, at their registered Singapore office unless one or more of the shareholders are Singapore residents. • Limited liability partnerships are not required to collect shareholder information on partners who are bodies corporate.
34. Legal arrangements – beneficial owners	PC	• While competent authorities have powers to access information on beneficial ownership in trusts, availability of that information is limited by the fact that only trusts administered by trustee companies and trust company service providers are obliged to maintain such information.
International Co-operation		
35. Conventions	LC	• The purpose elements required to prove third party money laundering are not in line with the Vienna and Palermo Conventions. • The scope of "terrorist act" does not fully cover all of the acts defined in Article 2(1) of the FT Convention.
36. Mutual legal assistance (MLA)	LC	• Singapore may not be able to freeze, seize and confiscate based on foreign orders against instrumentalities of crime, and their equivalent amounts, or instrumentalities "intended for use" in some cases of FT, ML, and predicate offences. • It is too soon to assess the effectiveness of the current MACMA (recently amended) and Singapore's responses to foreign countries seeking to become "prescribed" for case-by-case assistance. However, there remains one concern which existed under the previous regime: the requirement for more cumbersome procedures to obtain

		financial institution information than other types of information.
37. Dual criminality	C	• This Recommendation is fully observed.
38. MLA on confiscation and freezing	LC	• Singapore may not be able to freeze, seize and confiscate based on foreign orders against instrumentalities of crime, and their equivalent amounts, or instrumentalities "intended for use" in some cases of FT, ML, and predicate offences.
39. Extradition	C	• This Recommendation is fully observed.
40. Other forms of co-operation	C	• This Recommendation is fully observed.
Nine Special Recommendations	**Rating**	**Summary of factors underlying rating**
SR.I Implement UN instruments	LC	• The scope of "terrorist act" does not fully cover all of the acts defined in Article 2(1) of the FT Convention. • Provisions for obtaining access to frozen funds to pay basic expenses should be made specifically subject to the requirement of obtaining approval of the 1267 Committee for funds or other assets frozen as a result of S/RES/1267(1999) • The measures to implement S/RES/1373(2001) suffer from the following deficiencies: - Although Singapore relies on its well-honed procedures of advising its ministries and regulatory bodies of MHA's decisions to give effect to the actions initiated under the freezing mechanisms of other jurisdictions, or to designate persons in the context of S/RES/1373(2001), there is not a particularized legal framework for doing so. - While the majority of the FT Convention's provisions have been implemented, the scope of "terrorist act" does not fully cover all the acts defined in Article 2(1).
SR.II Criminalise terrorist financing	LC	• Not all of the offences in the Annex to the FT convention are terrorist acts in Singapore, an extra purpose requirement contravenes the Convention, and so financing of the Convention acts is not fully criminalised. • The effectiveness of the FT provisions has not been tested and cannot be assessed.
SR.III Freeze and confiscate terrorist assets	LC	• Although Singapore relies on its well-honed procedures of advising its ministries and regulatory bodies of MHA's decisions to give effect to the actions initiated under the freezing mechanisms of other jurisdictions, or to designate persons in the context of S/RES/1373(2001), there is not a particularized legal framework for doing so. There is no formal delisting procedure in place. • Provisions for obtaining access to frozen funds to pay basic expenses should be made specifically subject to the requirement of obtaining approval of the 1267 Committee for funds or other assets frozen as a result of S/RES/1267(1999). As Singapore has never utilized the TSOFA procedure for freezing, restraining, or forfeiting terrorist-related property, the efficiency and speed of this procedure has not been tested.
SR.IV Suspicious transaction reporting	C	• This Recommendation is fully observed.
SR.V International co-operation	LC	• The deficiencies identified in relation to R.36, also impact the rating for SR.V. • The deficiencies identified in relation to R.38, also impact the rating for SR.V. • There is only limited authority for Singapore to freeze, seize and confiscate instrumentalities of terrorism and terrorist financing at a foreign government's request, under Singapore's domestic provisions of TSOFA. • Outside of Commonwealth countries, Malaysia, and three treaty

		countries, extradition cannot be provided for FT offences not covered in the FT Convention (provision/collection of funds for a terrorist country or individual terrorist), unless they have been designated in the Gazette. The effectiveness of these provisions has not been demonstrated.
SR VI AML requirements for money/value transfer services	LC	• The risk of unlicensed MVTs is not fully addressed. • The limitations identified under Recommendation 5, 8, 10, 13, 14 and SR.VII also affect compliance with Special Recommendation VI.
SR VII Wire transfer rules	LC	• No explicit provision for record keeping where technical limitations prevent full originator information accompanying a cross-border transfer.
SR.VIII Non-profit organisations	LC	• Singapore has not yet conducted a TF vulnerability review of the NPO sector.
SR.IX Cross Border Declaration & Disclosure	LC	• Effectiveness: As the declaration system is very recent and only one month of statistics has been provided, its effectiveness and implementation across all agencies cannot yet be fully assessed.

TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1 & 2)	• The ML should be more effectively implemented by more aggressively pursuing the use of ML as a stand-alone offence, particularly in relation to third party money laundering activity, and the laundering of proceeds generated by foreign predicate offences. • Amend the third-party ML offences, sections 46(2) and 47(2), to remove the additional purpose elements for the offence of concealment or disguise, and provide for the additional alternative purpose element for the offence of conversion or transfer. • Ensure that sanctions are more effectively applied to both natural and legal persons convicted of money laundering.
2.2 Criminalisation of Terrorist Financing (SR.II)	• Amend the legislation to clearly cover the financing of all terrorist acts contained in the conventions and treaties that are listed in the Annex to the FT Convention. • Ensure that the apparent overlapping of provisions in the TSOFA, the UN (ATM) Regulations and the MAS (ATM) Regulations, which provide for different penalty regimes, does not negatively impact the effectiveness of the prosecutorial scheme, as terrorist financing prosecutions are brought forward. • Consider simplifying the framework of terrorist financing offences (*e.g.* by consolidating them into the TSOFA) in order to avoid inconsistencies and disparities in the sentencing and penalty framework.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Extend the restraint provisions to all instrumentalities and intended instrumentalities of crime, and "substitute property" for instrumentalities. • Pursue confiscation of frozen/seized assets more actively. • Streamline the procedure for obtaining bank records (by High Court order through application by the AGC) which is cumbersome compared to the procedure by which the police may simply seek a court order directly to obtain all other information. • Ensure that statistics distinguish between cases involving freezing/seizure and confiscation for ML and for predicate offences. • Consider amending the provisional restraint provisions under the CDSA to ensure that restraint may occur before a defendant is charged or informed that he/she will be charged, to avoid running the risk that assets will be depleted before they can be seized. • Consider whether using CPC's general powers for restraining property, rather than the existing powers in the CDSA, could present any future problems for retraining property relating to ML.
2.4 Freezing of funds used for terrorist financing (SR.III)	• Enact a legally-based mechanism to designate persons and organizations in the context of S/RES/1373(2001), which includes articulated standards by which any decision to designate or not designate may be judged. • Implement a particularised delisting procedure in relation to S/RES/1267. • In relation to unfreezing frozen assets pursuant to S/RES/1452(2002), specify procedures concerning the obligation to submit any proposed release of funds to the UN 1267 Committee for approval.
2.5 The Financial Intelligence Unit and its functions (R.26)	• Target more proactively the detection of money laundering cases, particularly those involving proceeds generated by foreign predicates,

	rather than focusing on identifying predicate offences. • Once STRO has refocused itself in this way, it should give consideration as to whether it has sufficient resources to manage this workload. • Strengthen the operational independence of the FIU to ensure that the current political commitment to the STRO's operations does not change with future governments. This should also include taking steps to ensure that the process of the police 'de-conflicting' STRs before they are analysed by the STRO does not undermine its independence as an FIU (i.e. by acting as a filter of the FIU's activities).
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• More pro-actively target and pursue ML investigations in general, and make more use of STRs to investigate ML cases, including the targeting of ML cases that are of a more international rather than domestic nature. • Once the law enforcement authorities begin focusing on these issues, they should consider whether they have allocated sufficient resources to manage this work.
2.7 Cross Border Declaration & Disclosure	• Due to the identified deficiencies in the disclosure regime, the authorities are recommended to make the new declaration system fully effective, ensuring that there is no confusion between coverage under the parallel disclosure and declaration systems. • Attention should be given to ensuring that the customs authorities are adequately resourced and trained in the implementation of this system across all forms of border control. • Ensure that implementation of the declaration system, and continued use of the disclosure system, has a focus on the detection of ML/FT.
3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	There are no recommendations for this section.
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	• Put the basic CDD obligations into law or regulation. • Move, as is currently planned, to cover commodities futures brokers for AML/CFT purposes (including comprehensive measures to cover R.5-8) as quickly as possible. • With regard to Recommendation 5, amend the AML/CFT notices to specify that reduced CDD measures are not allowed when there is a suspicion of ML/FT. MAS should also provide guidance about identifying possible linked transactions.
3.3 Third parties and introduced business (R.9)	• Clarify that financial institutions must immediately obtain all the necessary CDD information up front on introduced customers. • Ensure that commodities futures brokers are made subject to requirements in relation to Recommendation 9 as quickly as possible.
3.4 Financial institution secrecy or confidentiality (R.4)	• There are no recommendations for this section.
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	• Lay out the requirements for financial institutions to maintain business correspondence, and the requirement for money exchange and remittance businesses to in law or regulation. • Apply comprehensive record keeping provisions to commodities futures brokers. • Specify in the Notices that, where technical limitations prevent the full originator information accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.
3.6 Monitoring of transactions and relationships (R.11 & 21)	• Subject commodities futures brokers to requirements in relation to Recommendations 11 and 21.

	• Exercise enforceable powers to require financial institutions to apply additional AML/CFT counter-measures beyond normal obligations in relation to transactions with, or financial institutions from, countries that continue not to apply or insufficiently apply the FATF Recommendations.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	• Put certain aspects of the requirements (reporting to STRO, attempted transactions) into law or regulation. • Broaden the range of ML predicate offences to include human trafficking comprehensively, so as to ensure that the scope of the predicate offences for STR reporting is sufficient. • Subject money lenders and commodities futures brokers to adequate supervision for compliance with the reporting requirements. • Expand the CDSA tipping-off provisions to include not only those cases where a STR or related information has been reported but also is in the process of being reported to the FIU.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• Ensure that moneylenders effectively implement their obligations under R.15 going forward. • Subject moneylenders and commodities futures brokers to the requirements under Recommendation 22.
3.9 Shell banks (R.18)	• Consider expressly prohibiting the operation of shell banks.
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• Extend the fit and proper test to all senior management. • Develop more pro-active policies for assessing the risk of the unlicensed remittance sector with a view to reducing the number of possible money-changing and remittance businesses considering the large communities of migrant workers from countries with poor banking systems present in Singapore. • Commodities future brokers should be covered and adequately supervised as soon as possible. • Clarify the entry and inspection powers in relation to moneylenders to ensure that they may be exercised in contexts other than when there is a "reasonable suspicion" that there is a breach of the Moneylenders Act or rules.
3.11 Money value transfer services (SR.VI)	• Develop more pro-active policies with a view to reducing the number of possible unlicensed money-changing and remittance businesses considering the large communities of migrant workers from countries with poor banking systems present in Singapore.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• The Singapore authorities should adopt and implement comprehensive measures as contemplated in Recommendation 12 for real estate agents, dealers in precious metals and dealers in precious stones, accountants, and trust and company service providers (other than trust companies which are regulated as financial institutions). • As casinos come into operation, ensure that adequate AML/CFT requirements are applied to casinos as well. *Lawyers:* • Ensure that all of the basic obligations are contained in law and regulation. Enhance the CDD obligations by implementing requirements to: (a) Conduct CDD when there is a suspicion of ML/FT or when there are doubts about the veracity or adequacy of previously obtained customer identification data. (b) Identify the beneficial owner of all customers (not just for corporate customers). (c) Understand the ownership and control structure of the customer. (d) Understand the nature and purpose of the business relationship in all cases required by the FATF Recommendations.

	(e) Vonduct ongoing due diligence on the customer, and ensure that CDD information is kept up-to-date. (f) Broaden the categories of high risk customers to whom enhanced CDD measures must be applied. (g) Ensure that, at least, simplified CDD is applied to the low risk customers identified in the Rules. (h) Ensure that the ML risks are effectively managed when CDD cannot be completed at the start of the business relationship. (i) Ensure that, in all cases, if the lawyer is unable to obtain the required CDD information, he/she is not permitted to open the account/perform the transaction. (j) Consider making an STR if CDD cannot be satisfactorily completed. • In relation to Recommendation 6, require lawyers to conduct enhanced ongoing monitoring on relationships with clients who are PEPs. • In relation to Recommendation 9, implement a requirement to ensure that the intermediary/third party is regulated and supervised in accordance with the FATF Recommendations, and has measures in place to comply with Recommendations 5 and 10. • Implement a requirement to consider whether the intermediary/third party is located in a country that does not adequately apply the FATF Recommendations. A provision should also be enacted that explicitly states that the ultimate responsibility for customer identification and verification remains with the lawyer who is relying on the intermediary/third party. • In relation to Recommendation 10, implement requirements to maintain business correspondence, ensure that records are kept in such a manner as to permit the reconstruction of individual transaction, and ensure that all records can be made available on a timely basis. • In relation to Recommendation 11, implement a requirement that all findings relating to unusual transactions be kept for five years. • Ensure that the legal sector effectively implements the new requirements in relation to R.5, 6 and 8-11.
4.2 Suspicious transaction reporting (R.16)	• Conduct more outreach to DNFBPs to enhance compliance with the reporting obligation. • Issue relevant AML/CFT preventive measures to the various sectors still lacking them. Once introduced, intensive training efforts should be made. • Rectify the deficiencies relating to its tipping off provisions. • Adopt more comprehensive requirements for R.15 and R.21 for all DNFBPs. • Extend The Practice Direction of the Legal Profession to include the obligation of staff training to TF. Introduce provisions for screening procedures for employees.
4.3 Regulation, supervision and monitoring (R.24-25)	• Implement comprehensive AML/CFT obligations for real estate agents, dealers in precious metals and stones, accountants, and trust and company service providers (other than trust companies which are regulated as financial institutions), and ensure that these sectors are subject to an effective AML/CFT oversight mechanism. • Implement a more comprehensive mechanism to monitor lawyers for a broader range of AML/CFT measures. • When developing its casino sector, ensure that the regulations it will issue are comprehensive and subject to adequate supervision as well.
4.4 Other non-financial businesses and professions (R.20)	• Consider whether to continue issuing SGD 10 000 notes and/or develop requirements for when dealing with them.

5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• Broaden the requirements on beneficial ownership so that information on ownership/control is readily available in a timely manner.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• Broaden the requirements on beneficial ownership so that information on ownership/control for all trusts (not just those administered by trust companies) is readily available in a timely manner.
5.3 Non-profit organisations (SR.VIII)	• Conduct a TF vulnerability review of the NPO sector. • Accompany the current published guidance with outreach to the sector either by the Commissioner or through the Sector Administrators with further and more detailed information.
6. National and International Co-operation	
6.1 National co-operation and coordination (R.31)	• There are no recommendations for this section.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Amend the third-party ML offences, sections 46(2) and 47(2), to remove the additional purpose elements for the offence of concealment or disguise, and provide for the additional alternative purpose element for the offence of conversion or transfer. • Amend the offence of acquisition, possession or use to remove the additional element of proof (that the defendant acquired the property for no or inadequate consideration). • Amend the legislation to clearly cover the financing of all terrorist acts contained in the conventions and treaties that are listed in the Annex to the FT Convention. • In relation to unfreezing frozen assets pursuant to S/RES/1452(2002), specify procedures concerning the obligation to submit any proposed release of funds to the UN 1267 Committee for approval.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• Consider taking the initiative in making positive steps to inform foreign governments, particularly its neighbours in the Pacific Rim and Southeast Asia regions, that it may now provide a wide spectrum of mutual assistance, and the manner in which that assistance may be sought. • Change the definition of "instrumentality order" to include instrumentalities of all "serious offences" under the CDSA, and include instrumentalities "intended for use" in FT, ML, and predicate offences.
6.4 Extradition (R.39, 37 & SR.V)	• There are no recommendations for this section.
6.5 Other Forms of Co-operation (R.40 & SR.V)	• There are no recommendations for this section.
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• Statistics relating to the number of cases and amounts of property frozen, seized and confiscated should specifically distinguish between cases in which there is a close relation between the domestic predicate offences and the money laundering investigations. • Maintain statistics concerning the volume of international wire transfers.
7.2 Other relevant AML/CFT measures or issues	• There are no recommendations for this section.
7.3 General framework – structural issues	• There are no recommendations for this section.

TABLE 3: AUTHORITIES' RESPONSE TO THE EVALUATION

RELEVANT SECTIONS AND PARAGRAPHS	COUNTRY COMMENTS
Section 2.1, Paragraphs 107, 110, 111, 115 (low ML conviction)	Singapore's view is that a low number of ML convictions does not automatically equate to ineffective implementation. Singapore has always been tough on crime. In fact, the lower number of ML conviction is a sign of effectiveness as it is an indication of a successful crime prevention regime Our approach is to prevent as far as possible criminal activity from taking place, and robust law enforcement when criminal activity does take place. This applies to all crimes, including ML. This has resulted in Singapore having one of the lowest crime rates in the world.
Section 2.1, Paragraph 110, 115 (not aggressively pursuing foreign predicate linked ML)	In pursuing ML for foreign predicate offences, we need to have information on the underlying predicate offence, which is typically in the possession of foreign authorities. There must be some nexus between money in Singapore and the foreign predicate offence to prove the ML charge in Singapore, even though we do not require a formal conviction by the foreign country for it. The FIU has been very proactive in contacting its foreign counterparts in our attempts to establish the existence of a foreign predicate offence in cases involving suspicious inflows of funds into Singapore. Between 2004 and 14 November 2007, there were 247 instances where the FIU proactively contacted its foreign counterparts for this purpose. Typically, the FIU provides its counterparts with its analysis of suspicious funds flows, the particulars of suspects or potential suspects, and reasons why the funds flows were deemed suspicious. However, of all the replies received by the FIU, only 7 were positive. In these 7 cases, the FIU referred the matter to the Financial Investigation Branch for full ML investigations. We have since established that the accused persons are either at large or imprisoned in their home countries for the foreign predicate offence. Hence Singapore is unable to prosecute them at this time. However, our investigations have been kept open pending the arrest of the persons at large and/or a successful repatriation of the criminal proceeds.
Section 2.1. Paragraph 116 (ML as ancillary offence)	We do not regard ML as an ancillary offence, or a crime of lesser importance. We have set up the Financial Investigation Division (FID) that is specifically responsible for AML/CFT investigations. Moreover we have also a number of "self-laundering" prosecutions, and this shows that we will pursue <u>both</u> ML offences and domestic predicate offences, whenever there is evidence to support the charges.
Section 2.5. Paragraphs 223, 243 (Focus on Predicate Offence)	STRO has always focused on the detection of ML. This priority has been shared with all STRO officers and is translated in the 247 spontaneous disclosures made to its counterparts to try to pursue a ML offence pursuant to a foreign predicate, as well as the 233 requests for assistance to try to further a local (ML) investigation between 2004 and 14 November 2007. Additionally, STRO has also participated actively in awareness creation within enforcement agencies to avail them of STRO's capabilities as well as creating an adequate awareness in pursuing ML offences. The present results seem to indicate more positive success in the detection of predicate offences rather than ML, but STRO's has placed equal emphasis on both aspects.
Section 2.6, Paragraphs 276, 280 (Low number of ML investigations)	The Financial Investigation Division (FID), which comprises the Financial Investigation Branch (FIB), the Proceeds of Crime Unit (PCU) and the Suspicious Transaction Reporting Office (STRO) is specifically responsible for AML/CFT investigations. The number of full money laundering investigations conducted by the

RELEVANT SECTIONS AND PARAGRAPHS	COUNTRY COMMENTS
	FIB and PCU has been increasing over the years. This is due to a variety of factors, including an expansion of the schedule of money laundering predicate offences since 2004, as well as other efforts to proactively detect ML. There have also been a number of 3rd party ML investigations with respect to ML arising from foreign predicate offences. The majority of these investigations were initiated by FID from STR information. As such, it is Singapore's view that significant attention has been paid in conducting ML investigations, whether they arose out of a complaint or a STR, and regardless of whether there is a clear indication to a predicate offence. An ML investigation would be conducted as long as the facts of the case warrant it.
Section 2.6, Paragraph 279(c) (Recording of ML convictions/prosecutions)	Where ML had occurred in Singapore in respect of foreign predicate offences, a ML investigation may be conducted in Singapore. However, our investigations have shown that the perpetrators of ML and the predicate offences are usually based overseas and/or are at large. If they are based overseas, they would either be under investigation or imprisoned for the foreign predicate offence. In such situations, we would not be able to charge the perpetrators in court in Singapore for the ML offences. This explains our low conviction figures for ML arising from foreign predicate offences.

ANNEXES

ANNEX 1: ACRONYMS AND ABBREVIATIONS

ACRONYM OR ABBREVIATION	DESCRIPTION
ACCORD	ASEAN and China Cooperative Operations in Response to Dangerous Drugs
ACRA	Accounting and Corporate Regulatory Authority
AG	Attorney-General
AGC	Attorney-General's Chambers
AIO	Assistant Investigation Officer
AML/CFT	Anti-money laundering and counter-financing of terrorism
AMLA	Administration of Muslim Law Act
APO	Assistant planning officer
ASEAN	Association of Southeast Asian Nations
ASOD	ASEAN Senior Officials on Drug Matters
ATM	Automatic Teller Machine
BR Regs	Business Registration Regulations
BRA / BR Act	Business Registration Act
CA	Companies Act
CAD	Commercial Affairs Department
CAO	Commercial Affairs Officers
CBNI	Currency and Bearer Negotiable Instruments
CCA	Casino Control Act
CDD	Customer Due Diligence
CDP	The Central Depository
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
CEP	Community Engagement Program
CIS	Collective Investment Scheme
CMI	Capital Market Intermediaries
CNB	Central Narcotics Bureau
COC	Commissioner of Charities
CPAB	Crime Pattern Analysis Branch
CPC	Criminal Procedure Code
CPI	Corruption Perception Index
CPIB	Corrupt Practices Investigation Bureau

ACRONYM OR ABBREVIATION	DESCRIPTION
CRA	Casino Regulatory Authority
CRO	Criminal Records Office
DNFBP	Designated Non-Financial Businesses and Professions
EA	Evidence Act
EC	Essential Criterion
EFTPOS	Electronic Funds Transfers at Points of Sale Terminals
EXALT	External Liaison Team
FATF	Financial Action Task Force
FI	Financial Institution
FIB	Financial Investigation Bureau
FID	Financial Investigation Division
FIO	Financial investigation officer
FIT	Financial Investigation Team
FIU	Financial Intelligence Unit
HONLEA	Heads of National Drug Law Enforcement Agencies, Asia and Pacific
IAC	Inter-agency Committee on Anti-Money Laundering/Countering the Financing of Terrorism
IBG	Interbank GIRO
ICA	Immigration and Checkpoint Authority
ICPAS	Institute of Certified Public Accountants of Singapore
IDEC	International Drug Enforcement Conference
IDPU	Investigation Development and Planning Unit
IECC	International Economic Crime Course
IMC	Inter-Ministry Committee on Terrorism
IPC	Institutions of a Public Character
IRAS	Inland Revenue Authority of Singapore
ISD	Internal Security Department
JI	Jemaah Islamiyah
KYC	Know-Your-Client
LawSoc	The Law Society of Singapore
LLP	Limited Liability Partnership
LLP Regs	Limited Liability Partnership Regulations
LLPA	Limited Liability Partnership Act
MACMA	Mutual Assistance in Criminal Matters Act
MAS	Monetary Authority of Singapore
MAS(ATM) Regs	MAS (Anti-Terrorism Measures) Regulations

ACRONYM OR ABBREVIATION	DESCRIPTION
MCRBA	Money-changing and Remittance Businesses Act
MCYS	Ministry of Community Development, Youth and Sports
MDA	Misuse of Drugs Act
MFA	Ministry of Foreign Affairs
MHA	Ministry of Home Affairs
MICA	Ministry of Information, Communication and the Arts
MinLaw	Ministry of Law
ML	Money Laundering
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MOE	Ministry of Education
MOF	Ministry of Finance
MOH	Ministry of Health
MOM	Ministry of Manpower
MTI	Ministry of Trade and industry
MUIS	Majlis Ugama Islam Singapura
NCSS	National Council of Social Service
NSCS	National Security Coordination Secretariat
OSA	Official Secrets Act
PA	People's Association
PAOC	Public Accountants Oversight Committee
PC	Penal Code
PCA	Prevention of Corruption Act
PCU	Proceeds of Crime Unit
PID	Police Intelligence Department
PIN	Personal Identification Number
PMP	Practise Monitoring Programme
PMSC	Practice Monitoring Sub-committee
RMP	Royal Malaysia Police
ROC	Rules of Court
SAP	Statement of Auditing Practice
SFA	Securities and Futures Act
SGX	Singapore Exchange Limited
SJA	Singapore Jewellers Association
SLA	Singapore Land Authority

ACRONYM OR ABBREVIATION	DESCRIPTION
SPF	Singapore Police Force
SPRING	Standards, Productivity and Innovation Board
SSA	Singapore Standard on Auditing
SSC	Singapore Sports Council
STR	Suspicious Transactions Report
STRO	Suspicious Transaction Reporting Office
STROLLS	STR On-Line Lodging System
TC Regs	Trust Companies Regulations 2005
TCA	Trust Companies Act
TF	Terrorist Financing
TFC	Terrorist Financing Convention
TSOFA	Terrorism (Suppression of Financing) Act
UN(ATM) Regs	United Nations (Anti-Terrorism Measures) Regulations
UNSCR	UN Security Council Resolution
WINGS	Web-based Intelligence Analytical and Graphical visualisation System

ANNEX 2: LIST OF GOVERNMENT AND PRIVATE SECTOR BODIES INTERVIEWED

Accounting and Corporate Regulatory Authority
AIA
Ameertech Remittance and Exchange Services
Association of Banks in Singapore
Attorney-General's Chambers
Casino Regulatory Authority
Central Narcotics Bureau
Charles Monat Associates
Citibank
Commercial Affairs Department
Commissioner of Charities
Corrupt Practices Investigation Bureau
DBS Bank
DBS Vickers Securitys (Singapore) Pte Ltd.
DP Bureau
Homefront Security Division
HSBC Trustee
Inland Revenue Authority of Singapore (Comptroller of Property Tax)
Institute of Certified Public Accountants Society
Law Society of Singapore
Lion Capital Management Ltd.
Ministry of Community Development, Youth and Sports
Ministry of Finance
Ministry of Foreign Affairs
Ministry of Home Affairs
Ministry of Law
Monetary Authority of Singapore
PricewaterhouseCoopers
Private sector dealers in precious metals and stones
Private sector real estate agents
Rajah and Tan
Singapore Accredited Estate Agencies
Singapore Exchange Limited
Singapore Jewellers Association
Steering Committee
Western Union Global Network

ANNEX 3: KEY LAWS, REGULATIONS AND OTHER MEASURES

Money laundering offences – Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA)

Assisting another to retain benefits of drug trafficking

43. —(1) Subject to subsection (3), a person who enters into, or is otherwise concerned in an arrangement, knowing or having reasonable grounds to believe that by the arrangement —

(a) the retention or control by or on behalf of another (referred to in this section as that other person) of that other person's benefits of drug trafficking is facilitated (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise); or

(b) that other person's benefits of drug trafficking —

(i) are used to secure funds that are placed at that other person's disposal, directly or indirectly; or

(ii) are used for that other person's benefit to acquire property by way of investment or otherwise, and knowing or having reasonable grounds to believe that that other person is a person who carries on or has carried on drug trafficking or has benefited from drug trafficking, shall be guilty of an offence.

(2) In this section, references to any person's benefits of drug trafficking include a reference to any property which, in whole or in part, directly or indirectly, represented in his hands his benefits of drug trafficking.

…

(5) Any person who commits an offence under this section shall be liable on conviction to a fine not exceeding USD 200 000 or to imprisonment for a term not exceeding 7 years or to both.

Assisting another to retain benefits from criminal conduct

44. —(1) Subject to subsection (3), a person who enters into or is otherwise concerned in an arrangement, knowing or having reasonable grounds to believe that, by the arrangement —

(a) the retention or control by or on behalf of another (referred to in this section as that other person) of that other person's benefits of criminal conduct is facilitated (whether by concealment, removal from jurisdiction, transfer to nominees or otherwise); or

(b) that other person's benefits from criminal conduct —

(i) are used to secure funds that are placed at that other person's disposal, directly or indirectly; or

(ii) are used for that other person's benefit to acquire property by way of investment or otherwise, and knowing or having reasonable grounds to believe that that other person is a person who engages in or has engaged in criminal conduct or has benefited from criminal conduct shall be guilty of an offence.

(2) In this section, references to any person's benefits from criminal conduct include a reference to any property which, in whole or in part, directly or indirectly, represented in his hands his benefits from criminal conduct.

…

(5) Any person who commits an offence under this section shall be liable on conviction to a fine not exceeding USD 200 000 or to imprisonment for a term not exceeding 7 years or to both.

Concealing or transferring benefits of drug trafficking

46. —(1) Any person who —

(a) conceals or disguises any property which is, or in whole or in part, directly or indirectly, represents, his benefits of drug trafficking; or

(b) converts or transfers that property or removes it from the jurisdiction, shall be guilty of an offence.

(2) Any person who, knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits of drug trafficking —

(a) conceals or disguises that property; or

(b) converts or transfers that property or removes it from the jurisdiction, for the purpose of assisting any person to avoid prosecution for a drug trafficking offence or a foreign drug trafficking offence or the making or enforcement of a confiscation order shall be guilty of an offence.

(3) Any person who, knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits of drug trafficking, acquires that property for no or inadequate consideration shall be guilty of an offence.

(4) In subsections (1) (a) and (2) (a), references to concealing or disguising any property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

(5) For the purposes of subsection (3), consideration given for any property is inadequate if its value is significantly less than the market value of that property, and there shall not be treated as consideration the provision for any person of services or goods which are of assistance to him in drug trafficking.

(6) Any person who commits an offence under this section shall be liable on conviction to a fine not exceeding USD 200 000 or to imprisonment for a term not exceeding 7 years or to both.

Concealing or transferring benefits of criminal conduct

47. —(1) Any person who —

(a) conceals or disguises any property which is, or in whole or in part, directly or indirectly, represents, his benefits from criminal conduct; or

(b) converts or transfers that property or removes it from the jurisdiction, shall be guilty of an offence.

(2) Any person who, knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits from criminal conduct —

(a) conceals or disguises that property; or

(b) converts or transfers that property or removes it from the jurisdiction, for the purpose of assisting any person to avoid prosecution for a serious offence or a foreign serious offence or the making or enforcement of a confiscation order shall be guilty of an offence.

(3) Any person who, knowing or having reasonable grounds to believe that any property is, or in whole or in part, directly or indirectly, represents, another person's benefits from criminal conduct, acquires that property for no or inadequate consideration, shall be guilty of an offence.

(4) In subsections (1) (a) and (2) (a), references to concealing or disguising any property include references to concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

(5) For the purposes of subsection (3), consideration given for any property is inadequate if its value is significantly less than the market value of that property, and there shall not be treated as consideration the provision for any person of services or goods which are of assistance to him in criminal conduct.

(6) Any person who commits an offence under this section shall be liable on conviction to a fine not exceeding USD 200 000 or to imprisonment for a term not exceeding 7 years or to both.

Terrorist Financing offences – Terrorism (Suppression of Financing) Act (TSOFA)

Prohibition against providing or collecting property for terrorist acts

3. Every person who 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, in whole or in part, in order to commit any terrorist act,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 10 years or to both.

Prohibition against provision of property and services for terrorist purposes

4. Every person who directly or indirectly, collects property, provides or invites a person to provide, or makes 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, in whole or in part, 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, in whole or in part, they will be used by or will benefit any terrorist or terrorist entity,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding USD 100 000 or to imprisonment for a term not exceeding 10 years or to both.

Prohibition against use or possession of property for terrorist purposes

5. Every person who —

(a) uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out any terrorist act; or

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

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding USD 100 000 or to imprisonment for a term not exceeding 10 years or to both.

Prohibition against dealing with property of terrorists

6. —(1) 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 or controlled by or on behalf of any terrorist or terrorist entity, including funds derived or generated from property owned or 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.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding USD 100 000 or to imprisonment for a term not exceeding 10 years or to both.

(3) Any person who acts reasonably in taking, or omitting to take, measures to comply with subsection (1) shall not be liable in any civil proceedings arising from having taken or omitted to take the measures, if the person took all reasonable steps to satisfy himself that the relevant property was owned or controlled by or on behalf of any terrorist or terrorist entity.

AML/CFT requirements for banks – MAS Notice 626

1 INTRODUCTION

1.1 This Notice is issued pursuant to section 55 of the Banking Act (Cap. 19) and applies to all banks in Singapore.

1.2 This Notice (except for Paragraph 9) shall take effect on 1 March 2007. Paragraph 9 shall take effect on 1 July 2007. The earlier notice dated 11 November 2002 on the same subject is cancelled with effect from 1 March 2007.

2 DEFINITIONS

2.1 For the purposes of this Notice

"AML/CFT" means anti-money laundering and countering the financing of terrorism;

"beneficial owner", in relation to a customer of a bank, means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporate;

"business relations" means the opening or maintenance of an account by the bank in the name of a person and the undertaking of transactions by the bank for that person on that account;

"company" includes a body corporate formed or established outside Singapore under the law of the country or jurisdiction;

"CDD measures" or "customer due diligence measures" means the process of identifying the customer and obtaining information required by paragraph 4;

"customer", in relation to a bank, means a person in whose name an account is opened or intended to be opened, or for whom the bank undertakes or intends to undertake any transaction without an account being opened;

"FATF" means the Financial Action Task Force;

"government entity" means a government of a country or jurisdiction, a ministry within such a government, or an agency specially established by such a government through written law;

"STR" means suspicious transaction report; and

"STRO" means the Suspicious Transactions Reporting Office, Commercial Affairs Department of the Singapore Police Force.

2.2 A reference to any threshold or value limit expressed in S$ shall include a reference to the equivalent amount expressed in any other currency.

2.3 A reference to the completion of CDD measures is a reference to the situation when the bank has received satisfactory responses to all inquiries.

2.4 Unless the context otherwise requires, a reference to a financial institution supervised by the Authority does not include a person who is exempted from licensing, approval or regulation by the Authority.

3 UNDERLYING PRINCIPLES

3.1 This Notice is based on the following principles, which shall serve as a guide for all banks in the conduct of their operations and business activities:

(a) A bank must exercise due diligence when dealing with customers, persons appointed to act on the customer's behalf and beneficial owners.

(b) A bank must conduct its business in conformity with high ethical standards, and guard against undertaking any transaction that is or may be connected with or may facilitate money laundering or terrorist financing.

(c) A bank should, whenever possible and to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore in preventing money laundering and terrorist financing.

4 CUSTOMER DUE DILIGENCE

Anonymous or Fictitious Account

4.1 No bank shall open or maintain anonymous accounts or accounts in fictitious names.

When CDD measures are to be Performed

4.2 A bank shall perform CDD measures in accordance with this Notice when

(a) the bank establishes business relations with any customer;

(b) the bank undertakes any transaction of a value exceeding S$20 000 for any customer who has not otherwise established business relations with the bank;

(c) there is a suspicion of money laundering or terrorist financing, notwithstanding that the bank would otherwise not be required by this Notice to perform CDD measures; or

(d) the bank has doubts about the veracity or adequacy of any information previously obtained.

CDD Measures where Business Relations are Established

(I) Identification of Customers

4.3 A bank shall identify each customer who applies to the bank to establish business relations.

4.4 For the purpose of paragraph 4.3, a bank shall obtain and record information of the customer, including but not limited to the following:

(a) Full name, including any aliases;

(b) Unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

(c) Existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);

(d) Date of birth, incorporation or registration (as may be appropriate); and

(e) Nationality or place of incorporation or registration (as may be appropriate).

4.5 Where the customer is a company, the bank shall, apart from identifying the customer, also identify the directors of the company.

4.6 Where the customer is a partnership or a limited liability partnership, the bank shall, apart from identifying the customer, also identify the partners.

4.7 Where the customer is any other body corporate or unincorporate, the bank shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporate.

(II) Verification of Identity

4.8 A bank shall verify the identity of the customer using reliable, independent sources.

4.9 A bank shall retain copies of all reference documents used to verify the identity of the customer.

(III) Identification and Verification of Identity of Natural Persons Appointed to Act on the Customer's Behalf

4.10 Where the customer appoints one or more natural persons to act on his behalf in establishing business relations with the bank or the customer is not a natural person, a bank shall

(a) identify the natural persons that act or are appointed to act on behalf of the customer;

(b) verify the identity of these persons using reliable, independent sources; and

(c) retain copies of all reference documents used to verify the identity of these persons.

4.11 A bank shall verify the due authority of such persons to act on behalf of the customer.

4.12 A bank shall verify the due authority of such persons to act by obtaining, including but not limited to the following:

(a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and

(b) the specimen signatures of the persons appointed.

4.13 Where the customer is a Singapore government entity, the bank shall only be required to obtain such information as may be required to confirm that the customer is a Singapore government entity as asserted.

(IV) Identification and Verification of Identity of Beneficial Owners

4.14 Subject to paragraph 4.17, a bank shall inquire if there exists any beneficial owner in relation to a customer.

4.15 Where there is one or more beneficial owner in relation to a customer, the bank shall take reasonable measures to obtain information sufficient to identify and verify the identities of the beneficial owner.

4.16 Where the customer is not a natural person, the bank shall take reasonable measures to understand the ownership and control structure of the customer.

4.17 A bank shall not be required to inquire if there exists any beneficial owner in relation to a customer that is

(a) a Singapore government entity;

(b) a foreign government entity;

(c) an entity listed on the Singapore Exchange;

(d) an entity listed on a stock exchange outside of Singapore that is subject to regulatory disclosure requirements;

(e) a financial institution supervised by the Authority (other than a holder of a money changer's licence or a holder of a remittance licence, unless specifically notified by the Authority);

(f) a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or

(g) an investment vehicle where the managers are financial institutions

(i) supervised by the Authority; or

(ii) incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, unless the bank suspects that the transaction is connected with money laundering or terrorist financing.

4.18 For the purposes of paragraphs 4.17(f) and 4.17(g)(ii), a bank shall document the basis for its determination that the requirements in those paragraphs have been duly met.

(V) Information on the Purpose and Intended Nature of Business Relations

4.19 A bank shall obtain from the customer, when processing the application to establish business relations, information as to the purpose and intended nature of business relations.

(VI) Ongoing Monitoring

4.20 A bank shall monitor on an ongoing basis, its business relations with customers.

4.21 A bank shall, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the bank's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

4.22 A bank shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

4.23 A bank shall, to the extent possible, inquire into the background and purpose of the transactions in paragraph 4.22 and document its findings with a view to making this information available to the relevant competent authorities should the need arise.

4.24 A bank shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

Non-Face-to-Face Verification

4.25 A bank shall put in place policies and procedures to address any specific risks associated with non-face-to-face business relationships or transactions.

4.26 A bank shall implement the policies and procedures referred to in paragraph 4.25 when establishing customer relationships and when conducting ongoing due diligence.

4.27 Where there is no face-to-face contact, the bank shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reliance on Identification and Verification Already Performed

4.28 When a bank ("acquiring bank") acquires, either in whole or in part, the business of another financial institution (whether in Singapore or elsewhere), the acquiring bank shall perform CDD measures on the customers acquired with the business at the time of acquisition except where the acquiring bank has

(a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and

(b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring bank as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring bank.

CDD Measures for Non-Account Holders

4.29 A bank that undertakes any transaction of a value exceeding S$20,000 for any customer who does not otherwise have business relations with the bank shall

(a) establish and verify the identity of the customer as if the customer had applied to the bank to establish business relations; and

(b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.

4.30 Where a bank suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in this Notice, the bank shall treat the transactions as a single transaction and aggregate their values for the purpose of this Notice.

Timing for Verification

4.31 Subject to paragraph 4.32 of this Notice, a bank shall complete verification of the identity of the customer and beneficial owner

(a) before the bank establishes business relations; or

(b) before the bank undertakes any transaction for a customer, where the customer does not have business relations with the bank.

4.32 A bank may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner if

(a) the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations; and

(b) the risks of money laundering and terrorist financing can be effectively managed by the bank.

4.33 Where the bank establishes business relations before verification of the identity of the customer or beneficial owner, the bank shall complete such verification as soon as is reasonably practicable.

Where CDD Measures are Not Completed

4.34 Where the bank is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of an STR.

Joint Account

4.35 In the case of a joint account, a bank shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the bank.

Existing Customers

4.36 A bank shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.

5 SIMPLIFIED CUSTOMER DUE DILIGENCE

5.1 Subject to paragraph 5.2, a bank may perform such simplified CDD measures as it considers adequate to effectively identify and verify the identity of the customer, a natural person appointed to act on the customer's behalf and any beneficial owner if it is satisfied that the risks of money laundering and terrorist financing are low.

5.2 No bank shall perform simplified CDD measures in relation to customers that are from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the Authority or by other foreign regulatory authorities.

5.3 A bank may perform simplified CDD measures in relation to a customer that is a financial institution supervised by the Authority (other than a holder of a money changer's licence or a holder of a remittance licence, unless specifically notified by the Authority).

5.4 Where the bank performs simplified CDD measures in relation to a customer, it shall document

(a) the details of its risk assessment; and

(b) the nature of the simplified CDD measures.

6 ENHANCED CUSTOMER DUE DILIGENCE

Politically Exposed Persons

6.1 For the purposes of paragraph 6

"politically exposed person" means

(a) a natural person who is or has been entrusted with prominent public functions in a foreign country;

(b) immediate family members of such a person; or

(c) close associates of such a person.

"prominent public functions" includes the roles held by a head of state, a head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state owned corporations, and senior political party officials.

6.2 A bank shall, in addition to performing CDD measures specified in paragraph 4, perform enhanced CDD measures in relation to politically exposed persons, including but not limited to the following:

(a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a politically exposed person;

(b) obtain approval from the bank's senior management to establish or continue business relations where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;

(c) establish, by appropriate and reasonable means, the source of wealth and source of funds of the customer or beneficial owner; and

(d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

Other High Risk Categories

6.3 A bank shall perform enhanced CDD measures in paragraph 6.2 for such other categories of customers, business relations or transactions as the bank may assess to present a higher risk for money laundering and terrorist financing.

6.4 A bank shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the Authority or other foreign regulatory authorities.

7 PERFORMANCE OF CDD MEASURES BY INTERMEDIARIES

7.1 Subject to paragraph 7.2, a bank may rely on an intermediary to perform the CDD measures in paragraph 4 of this Notice if the following requirements are met:

(a) the bank is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;

(b) the intermediary is not one on which banks have been specifically precluded by the Authority from relying;

(c) the information that the bank would be required or would want to obtain which is being obtained by the intermediary may be relayed to the bank by the intermediary without any delay; and

(d) the intermediary is able and willing to provide, without delay, upon the bank's request, any document obtained by the intermediary which the bank would be required or would want to obtain.

7.2 No bank shall rely on an intermediary to conduct ongoing monitoring of customers.

7.3 Where a bank relies on an intermediary to perform the CDD measures, it shall document the basis for its satisfaction that the requirements in paragraph 7.1(a) have been met except where the intermediary is a financial institution supervised by the Authority (other than a holder of a money changer's licence or a holder of a remittance licence).

7.4 For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the bank shall remain responsible for its AML/CFT obligations in this Notice.

8 CORRESPONDENT BANKING

8.1 Paragraph 8 applies to a bank in Singapore when it provides correspondent banking services in Singapore to another bank or financial institution that is operating outside Singapore.

8.2 For the purposes of paragraph 8

(a) "correspondent bank" means the bank in Singapore that provides or intends to provide correspondent banking services in Singapore;

(b) "cross-border correspondent banking" means correspondent banking services provided to a bank or financial institution that is operating outside Singapore;

(c) "payable-through account" means an account maintained at the correspondent bank by the respondent bank but which is accessible directly by a third party to effect transactions on its own behalf;

(d) "respondent bank" means the bank or financial institution outside Singapore to whom correspondent banking services in Singapore are provided; and

(e) "shell bank" means a bank incorporated, formed or established in a country or jurisdiction where the bank has no physical presence and which is unaffiliated to a regulated financial group.

8.3 A bank in Singapore shall perform the following measures when providing cross-border correspondent banking services

(a) assess the suitability of the respondent bank by taking the following steps:

(i) gather adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(ii) determine from any available sources the reputation of the respondent bank and, as far as practicable, the quality of supervision over the respondent bank, including where possible whether it has been the subject of money laundering or terrorist financing investigation or regulatory action; and

(iii) assess the respondent bank's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent bank operates;

(b) document the respective AML/CFT responsibilities of each bank; and

(c) obtain approval from the bank's senior management to provide new correspondent banking services.

8.4 Where the cross-border banking services involve a payable-through account, the correspondent bank shall be satisfied that

(a) the respondent bank has performed appropriate CDD measures at least equivalent to those specified in paragraph 4 on the third party having direct access to the payable-through account; and

(b) the respondent bank is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide customer identification information to the correspondent bank upon request.

8.5 The correspondent bank shall document the basis for its satisfaction that the requirements in paragraphs 8.3 and 8.4 are met.

8.6 No bank in Singapore shall enter into or continue correspondent banking relations with a shell bank.

8.7 A bank shall also take appropriate measures when establishing correspondent banking relations, to satisfy itself that its respondent banks do not permit their accounts to be used by shell banks.

9 WIRE TRANSFERS

9.1 Paragraph 9 shall apply to a bank in Singapore when it effects the sending of funds by wire transfer or when it receives funds by wire transfer on the account of a person but shall not apply to a transfer and settlement between the bank and another financial institution where the bank and the other financial institution are acting on their own behalf as the wire transfer originator and the beneficiary institution.

9.2 For the purposes of paragraph 9

"beneficiary institution" means the financial institution that receives the funds on the account of the wire transfer beneficiary;

"cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are in different countries or jurisdictions;

"intermediary institution" means the financial institution that is an intermediary in the wire transfer payment chain;

"ordering institution" means the financial institution that acts on the instructions of the wire transfer originator in sending the funds;

"wire transfer beneficiary" means the person to whom or for whose benefit the funds are sent; and

"wire transfer originator" means the person who initiates the sending of funds.

Responsibility of the Ordering Institution

(I) Identification and Recording of Information

9.3 Before effecting a wire transfer, every bank that is an ordering institution shall

(a) identify the wire transfer originator and verify his identity (if the bank has not already done so by virtue of paragraph 4); and

(b) record adequate details of the wire transfer so as to permit its reconstruction, including at least the date of the wire transfer, the type and amount of currency involved, the value date and the details of the wire transfer beneficiary and the beneficiary institution.

(II) Cross-border Wire Transfers Exceeding S$2,000

9.4 In a cross-border wire transfer where the amount to be transferred exceeds S$2,000, every bank which is an ordering institution shall include in the message or payment instruction that accompanies or relates to the wire transfer the following:

(a) the name of the wire transfer originator;

(b) the wire transfer originator's account number (or unique reference number assigned by the ordering institution where no account number exists); and

(c) the wire transfer originator's address, unique identification number, or date and place of birth.

(III) Domestic Wire Transfers

9.5 In a domestic wire transfer, every bank that is an ordering institution shall either

(a) include in the message or payment instruction that accompanies or relates to the wire transfer all of the originator information required to be included as if the transaction had been a cross-border wire transfer exceeding S$2,000; or

(b) include only the originator's account number (or unique reference number where no account number exists) but be in a position to make the remaining originator information available within 3 working days of a request being made by the beneficiary institution.

Responsibility of the Beneficiary Institution

9.6 A bank that is a beneficiary institution shall implement appropriate internal risk-based policies, procedures and controls for identifying and handling in-coming wire transfers that are not accompanied by complete originator information.

Responsibility of Intermediary Institution

9.7 A bank that is an intermediary institution shall, in passing onward the message or payment instruction, maintain all the required originator information with the wire transfer.

10 RECORD KEEPING

10.1 A bank shall prepare, maintain and retain documentation on all its business relations and transactions with its customers such that

(a) all requirements imposed by law (including this Notice) are met;

(b) any transaction undertaken by the bank can be reconstructed so as to provide, if necessary, evidence for prosecution of criminal activity;

(c) the relevant competent authorities in Singapore and the internal and external auditors of the bank are able to review the bank's transactions and assess the level of compliance with this Notice; and

(d) the bank can satisfy, within a reasonable time or any more specific time period imposed by law, any enquiry or order from the relevant competent authorities in Singapore for information.

10.2 Subject to paragraph 10.4 and any other requirements imposed by law, a bank shall, when setting its record retention policies, comply with the following document retention periods:

(a) a period of at least 5 years following the termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

(b) a period of at least 5 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

10.3 A bank may retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a Singapore court of law.

10.4 A bank shall retain records pertaining to a matter which is under investigation or which has been the subject of an STR for such longer period as may be necessary in accordance with any request or order from STRO or from other relevant competent authorities.

11 SUSPICIOUS TRANSACTIONS REPORTING

11.1 A bank shall keep in mind the provisions in the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and in the Terrorism (Suppression of Financing) Act (Cap. 325) that provide for the reporting to the competent authorities of transactions suspected of being connected with money laundering or terrorist financing, and implement appropriate internal policies, procedures and controls for meeting its obligations under the law, including the following:

(a) establish a single reference point within the organisation to whom all staff are instructed to promptly refer all transactions suspected of being connected with money-laundering or terrorist financing, for possible referral to STRO via STRs; and

(b) keep records of all transactions referred to STRO, together with all internal findings and analysis done in relation to them.

11.2 A bank shall submit reports on suspicious transactions (including attempted transactions) to STRO, and extend a copy to the Authority for information.

11.3 A bank shall consider if the circumstances are suspicious so as to warrant the filing of an STR and document the basis for its determination where

(a) the bank is for any reason unable to complete CDD measures; or

(b) the customer is reluctant, unable or unwilling to provide any information requested by the bank, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.

12 INTERNAL POLICIES, COMPLIANCE, AUDIT AND TRAINING

12.1 A bank shall develop and implement internal policies, procedures and controls to help prevent money laundering and terrorist financing and communicate these to its employees.

12.2 The policies, procedures and controls shall include, amongst other things, CDD measures, record retention, the detection of unusual and/or suspicious transactions and the obligation to make suspicious transaction reports.

12.3 A bank shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity, in formulating its policies, procedures and controls.

Group Policy

12.4 A bank that is incorporated in Singapore shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Singapore.

12.5 Where a bank has a branch or subsidiary in a host country or jurisdiction known to have inadequate AML/CFT measures (as determined by the bank for itself or notified to banks generally by the Authority or by other foreign regulatory authorities), the bank shall ensure that its group policy on AML/CFT is strictly observed by the management of that branch or subsidiary.

12.6 Where the AML/CFT requirements in the host country or jurisdiction differ from those in Singapore, the bank shall require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

12.7 Where the law of the host country or jurisdiction conflicts with Singapore law such that the overseas branch or subsidiary is unable to fully observe the higher standard, the bank's head office shall report this to the Authority and comply with such further directions as may be given by the Authority.

Compliance

12.8 A bank shall develop appropriate compliance management arrangements, including at least, the appointment of a management level officer as the AML/CFT compliance officer.

12.9 A bank shall ensure that the AML/CFT compliance officer, as well as any other persons appointed to assist him, has timely access to all customer records and other relevant information which they require to discharge their functions.

Audit

12.10 A bank shall maintain an audit function that is adequately resourced and independent, and which will be able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements.

Employee Hiring

12.11 A bank shall have in place screening procedures to ensure high standards when hiring employees.

Training

12.12 A bank shall take all appropriate steps to ensure that its staff (whether in Singapore or overseas) are regularly trained on

(a) AML/CFT laws and regulations, and in particular, CDD measures, detecting and reporting of suspicious transactions;

(b) prevailing techniques, methods and trends in money laundering and terrorist financing; and

(c) the bank's internal policies, procedures and controls on AML/CFT and the roles and responsibilities of staff in combating money laundering and terrorist financing.

ANNEX 4: LAWS, REGULATIONS AND OTHER MATERIAL THAT WAS PROVIDED BY SINGAPORE TO THE ASSESSMENT TEAM

Accountants Act

Accounting & Corporate Regulatory Authority (Cap 2A)

Administration of Muslim Law Act (Cap.3)

AG's Opinion - Status of Notices

AGC: Australia Letter on MLA

AGC: UK Letter on MLA

AGC: CJD Portal

AGC: International Co-Operation PowerPoint Presentation

AGC: Sanctions (Powerpoint Slide)

AGC: Rahmad - Charge

AGC: Newspaper Clipping

AGC: Statistics from CPIB for Information of FATF Assessors

AGC: Tay Boon Hua @ Ah Chai Gd SDJ

Appraisers & Housing Agents Act (Cap 16)

Banking Act (Cap.19)

Banking (Corporate Goverance) Regulations (S583 of 2005)

Business Registration Act (Cap. 32)

Casino Control Act 2006

CDSA Amendment Bill

CDSA Order 89A

CDSA Order 89B

Charities Act (Cap.37)

Charities (Fund-Raising Appeals for Foreign Charitable Purposes) Regulations (Sec48)

Charities (Registration of Charities) Regulations (S178 of 2007)

Common Gaming Houses Act (Cap.49)

Companies Act (Cap.50)

Computer Misuse Act (Cap 50a)

Corruption Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A) (CDSA)

Criminal Procedure Code (Cap 68)

Extradition Act

Extradition (Amendment of First Schedule) Notification (S476-2007)

Extradition (Commonwealth Countries) Declaration 2007

Extradition Declaration (S475-2007)

Finance Companies Act (Cap 108)

Financial Advisers Act (Cap. 110)

Financial Advisers Regulations 2002 (Cap109, Rg 1)

Government Instruction Manual (IM3B) - Contracts & Purchasing Procedures, Debarment of Contractors

Government Instruction Manual (IM3G) - Revenue & Contracting Procedures, Penalties & Debarment

Guideline No: TCA-G04: Guidelines of Scope of Regulation

Guidelines on Fit & Proper Criteria (MCG-G01)

Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism for Real Estate Agents (2007)

Guidelines to MAS Notice 314

Guidelines to MAS Notice 626

Guidelines to MAS Notice 824

Guidelines to MAS Notice 1014 on Prevention of Money Laundering & Countering The Financing Of Terrorism

Guidelines to MAS Notice 3001

Guidelines to MAS Notice FAA-N06

Guidelines to MAS Notice SFA04-N02

Guidelines to MAS Notice SFA13-N01

Guidelines to MAS Notice TCA-N03

Income Tax Act (Cap.134)

Insurance Act (Cap.142)

Interpretation Act (Cap.1)

Legal Profession Act (Cap.161)

Legal Profession (Professional Conduct) (Amendment) Rules 2007 S384-2007

Legal Profession (Professional Conduct) Rules

Limited Liability Partnerships Act (Cap 163A)

MAS: 2nd Reading Speech MAS Amendment Bill

MAS (Anti-Terrorism Measures) Regulations (S515 of 2002)

MAS Code of Conduct

MAS: Consolidation of Notices

MAS (Freezing of Assets of Persons - Democratic Republic Of Congo) Regulations 2006 (S155 of 2006)

MAS (Freezing of Assets of Former President of Liberia & Connected Persons) Regulations 2004 (S260 of 2004)

MAS (Freezing of Assets of Persons - Côte d'lvoire) Regulations 2006 (S154 of 2006)

MAS (Freezing of Assets of Persons - Iran) Regulations 2007 (S104 of 2007)

MAS (Freezing of Assets of Persons - Sudan) Regulations 2006 (S553 of 2006)

MAS' Framework for Impact and Risk Assessment Of Financial Institutions

MAS Notice 314 to Life Insurers – AML/CFT

MAS Notice 626 Notice to Banks – AML/CFT

MAS Notice 817 to Finance Companies

MAS Notice 824 to Finance Companies - AML/CFT

MAS Notice 1014 to Merchant Banks - AML/CFT

MAS Notice 3001 to Money Changers & Remittance - AML/CFT

MAS Notice 3002 to Holders of Money Changers Licence & Remittance Licence - Record Of Transactions

MAS Notice FAA-N06 to Financial Advisors - AML/CFT

MAS Notice SFA04-02 to Capital Markets - AML/CFT

MAS Notice SFA13-N01 to Approved Trustees - AML/CFT

MAS Notice TCA-N03 to Trust Companies - AML/CFT

MAS OPM 3IIA

MAS: Statistics on Sanctions (Confidential)

Misuse of Drugs Act (Cap.185)

Monetary Authority of Singapore Act (Cap. 186)

Money-Changing and Remittance Businesses Act (Cap.187)

Money-Changing and Remittance Businesses Regulations 2005 (S687 of 2005)

Mutual Assistance in Criminal Matters Act (Cap.190A)

National Registration Act (Cap 201)

Objectives and Principles of Supervision in Singapore (MAS)

Official Secrets Act (Cap213)

Order 89E - Rules of Court

Organisational Chart - MAS

Partnership Act (Cap 391)

Payment Systems (Oversight) Act 2006

Penal Code (Cap.224)

Police Force Act

Postal Services Act

Postal Services Regulations

Practice Direction 2 (2005) ACRA

Practice Direction of the (Law Soc) Council

Prevention of Corruption Act (Cap 241)

Securities & Futures Act (Cap 289)

Securities and Futures (Licensing and Conduct of Business) Regulations 2002

Securities and Futures (Licensing and Conduct of Business) Regulations 2002 (Amendments) (2003)

Securities and Futures (Licensing and Conduct of Business) Regulations 2002 (Amendments) (2005)

Singapore's AML/CFT Regime (Powerpoint Slides Include Presentation on IAG; Operational and Policy Cooperation)

Singapore Standard on Auditing SSA 230

Societies Act (Cap.311)

Statement of Auditing Practice 19 on Guidance to Auditors on Money Laundering and Terrorist Financing

Statutory Bodies & Government Companies (Protection of Secrecy) Act (Cap319)

STRO Report - 1st Issue

STRO Report - 2nd Issue

STRO Report - 3rd Issue

STRO Report - 4th Issue

Terrorism (Suppression of Financing) Act (Cap.325)

Trust Companies Act (Cap.336)

Trust Companies (Exemption) Regulations 2005

Trust Companies Regulations

Trustees Act

United Nations Act

United Nations (Anti-Terrorism Measures) Regulations

Western Union: LPMT

Western Union: MAS Notices

Western Union: Presentation to FATF

Western Union Presentation: Voyager (120907)