SINGAPORE NATIONAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT REPORT

2013

MOF
MINISTRY OF FINANCE
SINGAPORE

Monetary Authority of Singapore

Contents

Background

Money Laundering and Terrorist Financing

Money laundering (ML) is the act of obscuring the true origin of illicit funds and making them appear legitimate. The ML cycle can be broken down into three stages, namely: (i) Placement, where proceeds of crime are introduced into the financial system to relieve a criminal of his "dirty" assets; (ii) Layering, where the illicit funds are separated from their source to conceal their illegal origin, usually via complex and cross-border transactions; and (iii) Integration, where the illicit funds are returned to the criminal for his use and benefit. Given that a profit motive underlies most crimes, the effective combating of ML can deal a significant blow to criminal activities.

Terrorist financing (TF) is the act of soliciting, collecting or providing funds, from both legal and illicit sources, with the intention of supporting terrorist activities or organisations. While a money launderer's main aim is to conceal the source of funds, a terrorist financier aims mainly to conceal the use of funds.

With the expansion of both physical and electronic financial infrastructure, ML and TF activities are becoming increasingly sophisticated and difficult to detect. The ease with which money and valuables can now move across borders means that regulatory authorities and enforcement agencies within and among countries must be able to cooperate and coordinate effectively to address emerging risks.

Singapore's National Risk Assessment (NRA)

The NRA is a government-wide exercise that seeks to enhance and deepen our collective understanding of the ML/TF risks in the country. The NRA is conducted under the ambit of the Steering Committee[1] for combating ML/TF, which comprises the Permanent Secretary of the Ministry of Home Affairs (MHA), Permanent Secretary of the Ministry of Finance (MOF) and Managing Director of the Monetary Authority of Singapore (MAS). The senior level involvement and the significant resources invested demonstrate Singapore's strong commitment to combat ML/TF.

The NRA takes reference from the Guidance on National Money Laundering and Terrorist Financing Risk Assessment published by the Financial Action Task Force (FATF) in February 2013[2]. Methodologies adopted by other international bodies such as the World Bank[3] and the Asia/Pacific Group on Money Laundering (APG)[4] were also considered and incorporated where appropriate.

[1] The Steering Committee, established in 1999, sets Singapore's broad policy objectives for combating ML and TF. The Committee ensures that the various national agencies have effective mechanisms in place to enable them to cooperate and where appropriate, coordinate domestically with each other to strengthen Singapore's resilience against illicit activities.

[2] The FATF is an inter-governmental body established in 1989 currently comprising 36 members, with the participation of over 180 countries through a global network of FATF-style regional bodies. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system.

Please refer to FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment at http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

[3] The World Bank is an international financial institution founded in 1944 that provides loans to developing countries for capital programmes. The World Bank's goal is to end extreme poverty within a generation and to boost shared prosperity. It currently comprises 188 member countries.

[4] The APG is an autonomous and collaborative international organisation founded in 1997 in Bangkok, Thailand comprising 41 members, including Singapore (founding member) and a number of international and regional observers. It is recognised as one of eight FATF-style regional bodies. The APG Implementation Issues Working Group, in partnership with the World Bank and Bank Negara Malaysia, successfully piloted a Strategic Implementation Planning (SIP) Framework at a workshop in Kuala Lumpur, Malaysia (held from 1 to 4 April 2008). Both the World Bank and the Government of Canada provided funding in support of this workshop. The SIP Framework was presented and adopted by the APG Plenary in July 2008 as an APG policy document to be used on a voluntary basis by members. More information can be found at: http://www.apgml.org/implementation-issues/page.aspx?p=babc505b-d61d-403d-8596-438a249d0eed.

Singapore's approach to the assessment is wide-ranging, covering stakeholders and representatives from both the public and private sectors. This helps to facilitate comprehensive exchanges of views and analyses to allow for a consistent approach in assessing the levels of risks, controls and supervisory oversight in each sector. The key government agencies involved are:

- Accounting and Corporate Regulatory Authority
- Attorney-General's Chambers
- Commercial Affairs Department
- Council for Estate Agencies
- Corrupt Practices Investigation Bureau
- Casino Regulatory Authority
- Charities Unit
- Insolvency and Public Trustee's Office
- Ministry of Finance
- Ministry of Home Affairs
- Ministry of Law
- Monetary Authority of Singapore
- Majlis Ugama Islam Singapura
- Singapore Customs
- Urban Redevelopment Authority

Anti-money laundering and countering the financing of terrorism (AML/CFT) practitioners and experts in the private sector were also consulted for views. As part of the assessment process, industry surveys were sent to various sectors to collect additional information and statistics to complement existing data. Towards the end of the NRA exercise, industry focus groups were convened to validate the findings.

Executive Summary

Singapore has one of the lowest crime rates in the world[5]. Key contributory factors are strong laws, tough enforcement and efficient prosecution. Money laundering (ML) and terrorist financing (TF) risks have also been reduced with effective cross-border cooperation among the relevant agencies.

The bulk of Singapore's exposure to ML/TF risks arises from offences committed overseas. As an international transport hub and financial centre, Singapore is a potential transit point for illicit funds. Therefore, Singapore has an important part to play in the global effort against ML/TF. Singapore has been an active member of the Financial Action Task Force since its early years in 1992 and is a founding member of the Asia/Pacific Group on Money Laundering.

Purpose

Dealing with ML/TF requires a *national* response. A comprehensive interagency risk assessment is therefore an important step to better understand Singapore's vulnerabilities and to develop plans to deal with them. The purpose of this national risk assessment (NRA) is to take that first step to identify, understand, and assess the ML/TF risks in Singapore. It will also inform the prioritisation and allocation of resources to enhance our national anti-money laundering and countering the financing of terrorism (AML/CFT) regime. This regime includes laws and regulations, as well as supervisory and enforcement frameworks, that are appropriate to mitigate the risks.

This is Singapore's first NRA report, and its publication is intended to help private sector stakeholders to better understand the ML/TF risks in their own sectors, as well as other sectors that they have dealings with. This will allow them to better assess the adequacy of their internal AML/CFT controls in mitigating the risks identified, and to strengthen these controls where necessary. The public at large will also benefit from greater awareness of the ML/TF risks in Singapore.

Findings

Singapore's openness as an international transport hub and financial centre exposes it to inherent cross-border ML/TF risks. The more vulnerable sectors are those that are internationally-oriented and cash-intensive. These include retail and private banks, remittance agents, money-changers, internet-based stored value facility holders, corporate service providers, casinos and pawnbrokers.

Encouragingly, the assessment has found that authorities have, put or are in the process of putting in place, effective preventive measures. To better manage cross-border ML/TF risks, Singapore has established formal cooperation channels with other jurisdictions for both supervisory and law enforcement purposes, with additional focus on AML/CFT. This framework for international cooperation is continually being strengthened to tackle new and emerging threats.

Financial Sector

Singapore is ranked by the International Monetary Fund as one of 25 systemically important financial centres in the world. The large size of the financial sector, high volume of transactions, and wide international reach inevitably exposes Singapore to its share of ML/TF risks. The financial sector is regulated by the Monetary Authority of Singapore (MAS), which has put in place a robust preventive regime that combines tough licensing requirements, strict AML/CFT regulations, and rigorous supervision. Nonetheless, there are areas for further enhancement.

[5] According to data presented in the United Nations Office on Drugs and Crime's report on International Statistics on Crime and Justice, Singapore's crime rate is one of the lowest in the world. More information can be found at: http://www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf

Full banks face higher inherent risks, owing to their larger customer volumes and the international nature of their transactions. These banks offer a wide range of products and services, and serve a broad spectrum of corporate and individual customers, including higher-risk customers such as politically exposed persons. The private banking industry in Singapore has also grown significantly over the past decade, boosted by the rising wealth in Asia. This industry is traditionally associated with higher ML risk due to the more high-value and bespoke services that can be offered, which has warranted additional due diligence on customers. Overall, AML/CFT controls in banks are the most developed, but there is scope for improvement in the areas of trade finance and correspondent banking.

Remittance agents and money-changers are cash-intensive sub-sectors and have been identified as having higher ML/TF risks. Large amounts of physical cash, high numbers of walk-in, one-off, and overseas customers, as well as voluminous transactions, contribute to higher inherent ML/TF risks. The implementation of the AML/CFT obligations and control measures in these sub-sectors is generally not as robust as in banks, and MAS will continue to ensure that supervision and enforcement efforts are further stepped up to manage the inherent ML/TF risks.

With the increased use of online payments, internet-based stored value facility holders have also been identified as one of the higher-risk sub-sectors. The cross-border nature of most transactions and the challenges faced by internet-based stored value facility holders in verifying customer identities are clear red-flags. Unfortunately, the AML/CFT regulations, supervisory regime and control measures in this sub-sector are nascent, and global best practices and standards are still being developed. MAS is considering additional supervisory powers and AML/CFT requirements to mitigate the risks.

Non-Financial Sectors

The global spotlight of AML/CFT has traditionally been on the financial system, and this has resulted in strong AML/CFT controls in the financial sector. The non-financial sectors may in some cases have taken false comfort that financial sector due diligence is sufficient. In reality, due diligence within the financial sector has its limits and an effective AML/CFT regime requires both the financial and non-financial sector stakeholders to do their part.

In light of internationally recognised ML/TF typologies, corporate service providers (CSPs) have been identified as a sector with a higher level of risk owing to the companies that CSPs help to incorporate for international customers. While CSPs generally do not handle large amounts of cash, there is a risk that the companies that they help to incorporate may be abused by criminals to set up complex and opaque structures for illicit purposes. It has been identified that AML/CFT controls are needed in this sector and the Accounting and Corporate Regulatory Authority has proposed new legislation to regulate CSPs, which is expected to come into effect in 2014, to ensure that concerns relating to customer due diligence and beneficial ownership are adequately addressed.

The fast-growing pawnbrokers sector is another risk area where controls can be improved. Transactions in this sector are mainly cash-based and gold items make up 90% of all pledges. Although this sector is domestically-oriented and the individual loan amounts are generally small, debt repayment using illicit funds and pawning of stolen goods are channels of risk. The Insolvency and Public Trustee's Office plans to introduce an AML/CFT regime in the sector in 2014.

Gambling operations and the use of international market agents (IMAs)[6] have been known to be possible conduits through which illicit funds can be laundered. The casino sector's cash-intensive business exposes it to a higher level of inherent risks. The casino sector is relatively new in Singapore, having started only in 2010, but the AML/CFT controls have been found to be strong. The Casino Regulatory Authority of Singapore (CRA) will continue to enhance controls, regulation and supervision over the casinos and IMAs, where necessary, to ensure that AML/CFT measures are implemented effectively.

Emerging Risks

In the course of our risk assessment, a number of areas have been identified for further study, such as virtual currencies that are gaining wider acceptance as a means of payment[7]. There is currently no global standard on how virtual currencies should be treated. While regulators internationally are still grappling with this issue[8], the ML/TF risks continue to grow. Other areas identified are the precious stones and metals dealers sector, and the Singapore Freeport. We will be studying these further to better understand the relevant ML/TF typologies and international best practices for addressing these risks, and to determine whether any safeguards and mitigating measures are needed.

Conclusion

Given Singapore's status as an international transport hub and financial centre, the inherent ML/TF risks are high. At the same time, Singapore has in place a robust AML/CFT regime, grounded in tough regulations, rigorous supervision and effective enforcement, that has helped mitigate these risks. There are a few areas where controls need to be strengthened and efforts are underway to address these areas.

[6] An IMA is a person licensed by CRA who organises, promotes or facilitates the playing of any game in a casino by one or more patrons, for which the licensed IMA receives a commission or other forms of payment from the casino operator.

[7] At a US Senate Committee Hearing in November 2013, the US Department of Justice said that bitcoins can be "legal means of exchange", boosting prospects for wider acceptance of the virtual currency.

[8] On 5 December 2013, China's Central Bank said that its banks and payment systems are barred from handling bitcoins but private individuals are allowed to trade them at their own risk. However, the Bank of America Merrill Lynch, in its first research report on bitcoins, said the currency has potential to become a "major means" of payment.

1. Economic and Geographical Environment

Economic Environment

As a small country with no natural resources, Singapore has been externally-oriented since its colonial days. Sitting at the centre of a web of trade routes and connected to more than 600 ports in over 120 countries, it is a natural global trading and shipping hub[9].

Today, Singapore is a dynamic international trading, business and financial centre. Its diversified economy spans manufacturing, aviation and maritime transport, business and financial services, and tourism.

Manufacturing has been and remains a pillar of Singapore's economy. Singapore's skilled workforce and strong business environment, which includes political stability and a robust legal framework, have drawn thousands of multinational corporations to invest and establish a wide range of businesses centred on petrochemicals, pharmaceuticals and electronics.

However, the importance of services to the Singapore economy has grown substantially in recent decades. As at the end of 2012, the services industry contributed nearly two-thirds of the Gross Domestic Product (GDP) and employed 70% of the workforce. The business services sector, which includes legal, accounting and auditing services, is the largest sector after wholesale and retail trade.

Singapore has also built up a thriving financial centre that is host to more than 700 financial institutions (FIs) offering a wide variety of financial products and services. It manages assets from diverse sources and intermediates a significant volume of funds through a highly-developed financial system.

Singapore's tourism industry is also thriving, attracting over 10 million visitors annually. Two integrated resorts (IRs) – Marina Bay Sands and Resorts World Sentosa – commenced operations in 2010, providing a wide array of amenities and attractions to further boost the tourism industry. The IRs also marked the opening of Singapore's two casinos.

As an international business and financial centre with an open economy, Singapore is inevitably exposed to risks of regional and international ML/TF by wrongdoers seeking to exploit our economic openness, efficient financial system and well-developed business infrastructure.

[9] Please refer to: http://www.mpa.gov.sg/sites/maritime_singapore/what_is_maritime_singapore/premier_hub_port.page.

Geographical Environment

Located in Southeast Asia, Singapore is an island state with a land area of about 715 square kilometres. We are one of the smallest countries in the world, and the smallest in the region.

To the north of Singapore and connected by two link bridges is Johor, the third largest and one of the most developed states in Peninsula Malaysia. To the south, the key islands of the Riau Archipelago of Indonesia - Bintan and Batam - are a short ferry trip away. The bridges and ferry connections have facilitated trade and boosted two-way economic and people-to-people interaction.

Singapore's strategic geographical location has enabled us to develop into an international aviation and maritime transportation hub. Situated along the vital shipping lanes of the Straits of Malacca and Singapore, Singapore is one of the busiest ports in the world, connected to more than 600 ports in over 120 countries[10]. With an airport serving some 110 airlines flying to over 240 cities in about 60 countries and territories worldwide, Singapore serves as a major gateway to Southeast Asia[11].

Operational efficiency is important to manage and handle the high inflow and outflow of passengers and cargo through Singapore. However, like all global hubs, Singapore is vulnerable to being used as a transit point for criminal and terrorist activities. A strong border control system is thus integral in preventing criminal and terrorist elements from entering Singapore.

Political Environment

Corruption

Singapore adopts a zero-tolerance approach in tackling corruption. Singapore's anti-corruption framework is supported by strong political will and rests on four key pillars: (i) strong anti-corruption laws; (ii) an independent judiciary; (iii) a responsive public service; and (iv) effective enforcement.

The effective enforcement of anti-corruption laws by the independent Corrupt Practices Investigation Bureau (CPIB) has kept corruption levels low and under control. A specialised Financial Investigations Branch was established within CPIB in June 2011 to focus on investigating the laundering of corrupt or criminal proceeds in accordance with the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA).

CPIB investigates an average of around 200 corruption cases each year, a quarter of which relate to the public sector. Conviction rates for corruption cases prosecuted in court have remained above 95% since 2007. Singapore's ability in controlling corruption is also evident from its consistently high ratings in various corruption indices. For instance, in Transparency International's Corruption Perceptions Index 2012, Singapore was ranked 5th out of 176 countries. Singapore's quality of governance has also been rated positively by the World Bank's Worldwide Governance Indicators (2011), particularly for the Control of Corruption (96.2 percentile rank) and Government Effectiveness (99.1 percentile rank).

Overall, Singapore's robust national anti-corruption framework has helped to keep corruption at bay.

[10] Please refer to: http://www.mpa.gov.sg/sites/global_navigation/news_center/speeches/speeches_detail.page?filename=sp130926a.xml.

[11] Please refer to: http://www.changiairportgroup.com/cag/html/business-partners/

Terrorism

There is strong political will to fight terrorism and TF. Singapore has implemented a robust and integrated strategy to deter, detect and respond to terrorist incidents. The strategy has five layers – Intelligence and International Cooperation, Border Control, Target Hardening, Community Involvement, and Crisis and Consequence Management. There is also a comprehensive legal, policy and supervisory framework to deal with the threat of terrorism and to cooperate with the international community such as the United Nations (UN) in the fight against terrorism. The Steering Committee for combating ML/TF determines the broad policy objectives to fight TF.

Singapore is situated in a region where several terrorist groups operate actively and have carried out attacks in the last 10 years. Although Singapore has been fortunate enough not to have fallen victim to terrorist attacks in recent years, there is no let-up in our vigilance, and our political leaders continue to stress the importance of working together to strengthen our defences against the continuing threat.

Overall, our robust laws and the efforts of our law enforcement agencies have helped to keep the ML/TF risks arising from the political environment factors under control.

BOX ITEM 1A: COMMITMENT TO FIGHT TERRORISM AND TF

"Fortunately, Singapore has not suffered a terrorist attack in recent years... But the threat has not disappeared, and we remain a target. From time to time, we hear reports of terrorists in our region wanting to attack Singapore or Singapore assets in our neighbourhood. We must never let our guard down."

- Prime Minister Lee Hsien Loong
(Speech delivered at the International Conference on Terrorist Rehabilitation and Community Resilience in March 2013)

Singapore's strong commitment to fight terrorism and TF has not wavered over the years. To deal effectively with terrorism, the Government has adopted a multi-pronged approach comprising the following key elements:

Intelligence and International Cooperation

The Internal Security Department (ISD) is a specialised intelligence agency under MHA that collects and analyses intelligence in relation to all terrorism-related activities. ISD works closely with local agencies like the Singapore Police Force (SPF), the Commercial Affairs Department (CAD), the Immigration & Checkpoints Authority (ICA) and other relevant agencies to exchange information and intelligence on terrorism and TF matters. There are established work processes and communication channels to share information among the local agencies.

Singapore's security, intelligence and law enforcement agencies actively nurture and sustain long-established relationships with their foreign counterparts. After the September 11 attacks, intelligence sharing and cooperation with both regional and international intelligence agencies have been enhanced, and this has resulted in a number of tangible successes[12]. Singapore also actively supports and participates in Counter-Terrorism (CT) initiatives undertaken by regional fora such as the Association of Southeast Asian Nations (ASEAN), the Asia-Europe Meeting and the Asia-Pacific Economic Cooperation. These include mechanisms to enable cross-border exchange of information, intelligence sharing and capacity building.

Border Control

Stringent measures are in place to prevent terrorists and munitions, including weapons of mass destruction, from entering Singapore (for more details please refer to the section on Customs and Other Border Controls).

Target Hardening

This consists of deploying security measures to reduce the vulnerability of "at-risk" buildings to terrorist attacks. The Government also works with multiple stakeholders to educate and create awareness on good building security for all other facilities, particularly the soft targets (e.g. hotels and shopping malls).

Community Involvement

A cornerstone of our CT approach is sustained engagement of the public and the community in preventing the spread of terrorism and in building community resilience. This is achieved through our community engagement and outreach programmes that focus on building awareness and preparedness. The former involves instilling in the community a strong national identity, a sense of belonging and rootedness to the nation, and enhancing inter-racial and inter-religious understanding. The latter involves engaging the community on CT efforts.

Crisis and Consequence Management

Mitigation capabilities for non-conventional threats such as chemical, biological and radiological terrorism have been developed. A crisis management mechanism has also been put in place to handle such events.

Inter-Ministry Committee on Terrorist Designation

To strengthen Singapore's fight against TF, an Inter-Ministry Committee on Terrorist Designation has been established as the designated authority to implement terrorist designations, oversee the listing/delisting of terrorists, and coordinate the freezing/unfreezing of terrorist funds and assets in accordance with the relevant United Nations Security Council Resolutions (UNSCRs).

[12] For example, intelligence shared by ISD with its foreign counterparts led to the arrests of Al-Qaeda operative Mohammad Mansour Jabarah in Oman and Jemaah Islamiyah (JI) bomb-maker Fathur Rohman al-Ghozi (deceased) in the Philippines.

AML/CFT Institutional Environment

Government agencies in Singapore are generally equipped with adequate resources for effective AML/CFT supervision in their domains. Some sectors are still nascent. In these cases, the relevant authorities are calibrating the resources required to ensure that the regulatory regime can be implemented effectively.

There is strong interagency coordination and cooperation among relevant authorities in Singapore on AML/CFT matters. The Steering Committee for combating ML/TF ensures that the relevant authorities have effective mechanisms in place to enable them to cooperate and coordinate domestically with one another to strengthen Singapore's resilience against criminal abuse.

Additionally, other interagency mechanisms exist to facilitate domestic cooperation on AML/CFT matters such as the Inter-Ministry Committee for Export Controls, the Inter-Ministry Committee for Terrorism and the Inter-Ministry Committee for Terrorist Designation.

2. Legal, Judicial and Institutional Framework

Legislation and Enforcement

Singapore has put in place strong laws and regulations to punish crimes and protect our system, including the financial system, from being used to carry out illegal activities.

Singapore has a wide range of serious offences for which an ML charge can apply, i.e., predicate offences. The list of 424 serious offences includes the offences in the 21 categories designated by the Financial Action Task Force (FATF) and is reviewed regularly with a view to extend the crime of ML to a wider range of predicate offences. Our laws also allow for the seizure and confiscation of ill-gotten gains.

Singapore has also enacted domestic legislation that enables our law enforcement authorities to take swift and effective action against terrorists, terrorist entities and their supporters, including financiers of terrorism. Singapore is party to 10 out of 13 UN Counter-Terrorism Conventions and Protocols, and we are working towards acceding to the remaining Conventions.

BOX ITEM 2A: STRENGTHENING SINGAPORE'S AML/CFT LEGAL FRAMEWORK

Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act and Moneylenders Act

The CDSA is the primary legislation in Singapore that criminalises the laundering of criminal benefits and provides for the investigation and confiscation of such benefits. The penalty for the offence of ML is imprisonment of up to seven years and/or fine of up to a maximum of $500,000 for natural persons, and a maximum of $1 million for such offences committed by institutions/corporations. In February 2010, the CDSA was amended to address all the technical deficiencies identified in Singapore's third round of FATF Mutual Evaluation. In July 2013, the crime of ML was extended to cover more predicate offences such as serious tax offences. Another round of CDSA amendments is tentatively scheduled in 2014 to further strengthen our AML levers.

Additionally, the Moneylenders Act was amended in February 2010 to include, among others, a provision to target ML acts by abettors who help to launder the illicit proceeds of loansharks. With the amendment, the act of receiving, possessing, concealing or disposing of any funds or other property, or engaging in a banking transaction relating to any funds, on behalf of another person known or reasonably believed to be carrying on an unlicensed moneylending (UML) business in Singapore attracts a fine of between $30,000 to $300,000 and imprisonment of up to seven years for repeat offenders. The amendments to the Moneylenders Act, which *inter alia* aim to disrupt the activities that sustain UML operations, are part of our efforts to decisively contain crime, including ML, before they pose a serious threat to Singapore's safety and security.

Terrorism (Suppression of Financing) Act (TSOFA)

The TSOFA was enacted in 2002 to counter TF in Singapore. It also gives effect to the UN International Convention for the Suppression of the Financing of Terrorism (1999) and the UNSCR 1373 (2001), which call on states to work together to prevent and suppress acts of terrorism, including TF.

To strengthen the deterrent effect, the TSOFA was amended in August 2013 to raise the maximum penalties for TF offences, from $100,000 to $500,000 for individuals and $1 million for entities. The maximum imprisonment term remains unchanged at 10 years. The amended TSOFA also includes new provisions which: (i) make it an offence to disclose, by one person to another, information which is likely to prejudice the investigation of a TF offence; and (ii) protect the identity of informers against disclosure and discovery during legal proceedings. Overlapping provisions in the MAS (Anti-Terrorism Measures) Regulations and the UN (Anti-Terrorism Measures) Regulations were also migrated to the TSOFA, so as to simplify and streamline our CFT regime. Overall, the amendments serve to strengthen our CFT regime and further align it with the FATF Recommendations.

Law Enforcement Agencies

The Financial Investigation Group (FIG) of CAD is the lead enforcement authority for ML/TF investigations. Other law enforcement agencies may refer complex ML cases to FIG for investigation or consult FIG on other ML or financial investigations. FIG also provides training for law enforcement agencies on ML and financial investigations, and the tracing of criminal proceeds. As CPIB is the sole and independent law enforcement agency responsible for investigating offences under the Prevention of Corruption Act (PCA), CPIB separately leads ML investigations related to corruption cases including the confiscation of benefits derived from corrupt proceeds. These have led to an increase in the number of ML prosecutions and convictions.

FIG is stepping up its efforts to update existing processes and procedures to promulgate the conduct of proactive financial investigations in all cases related to major proceeds-generating offences.

ISD is the lead agency for all investigations into terrorism and terrorism-related offences. ISD works closely with FIG in investigating TF offences, including tracing the assets of the suspected terrorists to ensure that the assets are frozen in a timely manner.

Range of Powers

The law enforcement officers from SPF, CPIB and the Central Narcotics Bureau (CNB) have the powers to access all necessary documents and information for use in investigations, prosecutions and related actions. These include powers to use compulsory measures for the production of records, search of persons and premises, taking of statements, and seizure and confiscation of evidence and property involved.

In relation to TF investigations, officers of FIG are empowered under the TSOFA, CDSA and Criminal Procedure Code (CPC) to exercise a variety of investigative powers, including the powers of asset tracing, seizure and confiscation, and arrest.

Domestic Coordination

There is strong domestic coordination on both the investigation and intelligence fronts. As the main enforcement authority for ML/TF investigations, CAD works closely with the other SPF units and other law enforcement agencies such as CNB and CPIB, and participates in joint investigations. Relevant government authorities meet regularly at the working and management levels to keep one another abreast of the latest developments in crime trends. There are also regular meetings between CAD and the CT unit at the working and management levels to ensure that there are opportunities for sharing information, and coordinating policy decisions and implementation issues among relevant authorities. Interagency delegations also regularly participate in meetings of the FATF and the Asia/Pacific Group on Money Laundering (APG).

With regard to the sharing of financial intelligence, the Suspicious Transaction Reporting Office (STRO), as the Financial Intelligence Unit (FIU) of Singapore, maintains close working relationships with various enforcement and intelligence agencies, both domestically and internationally. STRO regularly disseminates financial intelligence to the respective agencies for necessary action, and also responds to requests from them. STRO also shares emerging crime trends and typologies with them.

Financial Intelligence Unit

STRO has been working with local law enforcement agencies to develop and enhance standard operating procedures on the use of financial intelligence for their investigations. While STRO has been successful in identifying domestic predicate offences through its analyses, it also pursues the identification of ML rigorously. There are specialised teams in STRO to focus on specific ML typologies and risks.

In particular, one of STRO's focus areas is pursuing ML from foreign predicate offences. STRO has devoted resources towards negotiating and signing Memoranda of Understanding (MOUs) with its foreign counterparts, especially with countries with developed or emerging financial centres. STRO is also increasing its spontaneous referrals to its foreign counterparts to increase the efficacy of detecting ML in Singapore of the proceeds of foreign predicate offences.

BOX ITEM 2B: OVERVIEW OF SUSPICIOUS TRANSACTION REPORTING REGIME

STRO was established formally on 10 January 2000 and is the main agency responsible for receiving and analysing suspicious transaction reports (STRs), as well as disseminating the results of the analyses to relevant law enforcement agencies.

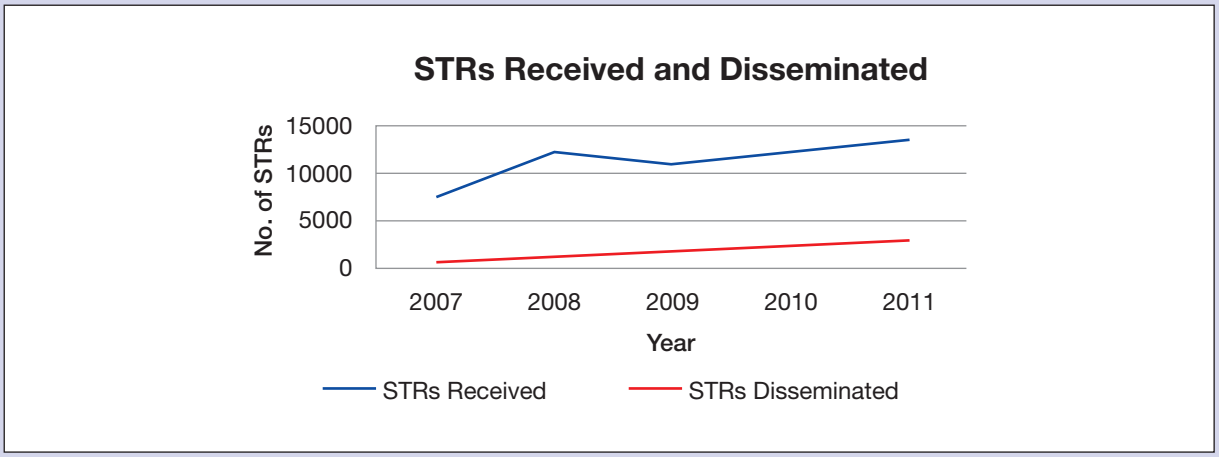
The statutory obligation to file STRs is enacted in the CDSA and may be supplemented by AML/CFT guidelines issued by regulators of the various sectors. Under the CDSA, any person has to lodge an STR with STRO if, in the course of his work, he has reason to suspect that any property is linked to crime. The lodging of STRs is governed by the tipping-off provision under the CDSA, where it is an offence for a person to disclose to another, information which is likely to prejudice an investigation or proposed investigation. Identities of the reporting entities are protected under the CDSA and the Official Secrets Act.

STRO proactively engages the industry and community to build a strong culture of STR filing. STRO regularly conducts public outreach to share crime typologies and the indicators of suspicious transactions, as well as provide feedback on STRs filed. This has translated into more than 13,000 STRs filed in 2011 by more than 19 sectors, including the FIs as well as designated non-financial businesses and professions (DNFBPs)[13] such as casinos and lawyers. The banking sector is the top STR filing sector and the casino sector is the leading sector among DNFBPs in filing STRs.

STR figures have to be understood and interpreted in the appropriate context, including but not limited to the coverage of the STRs reported, the ML/TF risks of the sector, the existing processes and structures to detect and prevent the misuse of the sector for ML/TF purposes and the usefulness of the information in detecting crime. Hence, while a higher number of STRs from a sector may be indicative of a higher level of vigilance, a lower number of STRs from another sector could be due to the specific business activities of the sector or lower ML/TF risks.

[13] FATF defines DNFBPs as: (i) Casinos; (ii) Real estate agents; (iii) Dealers in precious metals; (iv) Dealers in precious stones; (v) Lawyers, notaries and other independent legal professionals and accountants; and (vi) Trust and Company Service Providers. The full definition can be found in the General Glossary of the FATF Recommendations (February 2012).

Over the years, it is noted that the increase in STRs has been accompanied by STRs containing useful and comprehensive information that is used for STRO's analyses. All STRs are analysed and a significant number has been disseminated to various domestic law enforcement agencies and STRO's foreign counterparts for follow-up actions. In 2011, STRO disseminated about 20% of STRs it received. The chart below shows the number of STRs that were received and disseminated from 2007 to 2011.



STRs have been very useful in providing leads to ongoing investigations and for general intelligence relating to possible criminal activity, including ML/TF. STRs have also led to the commencement of ML investigations and convictions of money launderers.

Customs and Other Border Controls

A strong border control system is integral in preventing criminal and terrorist elements from entering Singapore. Safeguarding Singapore's borders is a multiagency effort which involves strict enforcement and close coordination among relevant border control agencies such as ICA, Singapore Customs, and the Police Coast Guard (PCG), and is supported by a comprehensive and robust legal framework and regime.

Border control agencies take a calibrated approach in carrying out their border security functions. Risk management techniques are adopted for both passenger and cargo clearance to facilitate legitimate travel and trade without compromising security. Technology is used to enhance effectiveness in security detection at the checkpoints. Our laws and regulations are also regularly reviewed to ensure that they remain effective and continue to meet international standards.

To prevent the entry of terrorists and smuggling of dangerous items such as weapons and explosives into Singapore, security was stepped up following the events of 11 September 2001 at the various entry points around the island. This included stringent checks on travellers, vehicles, baggage and cargo conducted at the sea, air and land checkpoints. There were increased patrols and other visible deterrence measures at the checkpoints area and the coastline. Visa requirements were also imposed on visitors from selected countries.

The challenges posed by a porous coastline are common to Singapore and our regional neighbours. To foster close cooperation to safeguard our coastline, Singapore works closely with our regional neighbours to exchange information on border security issues. Singapore also supports capacity building efforts in the region through the provision of training to enhance operational efficiency of other border control agencies, and joint initiatives to patrol regional waters to deter crime.

Overall, Singapore's openness to trade and immigration is balanced by strong border controls, effective interagency coordination and close cooperation with our regional neighbours to safeguard Singapore against ML/TF threats.

Declaration and Disclosure System

Singapore has established Free Trade Zones (FTZs) at the seaports and airports to facilitate entrepot trade. Customs and excise duties and Goods and Services Tax are suspended for goods deposited in a FTZ. These duties and taxes are payable upon removal from the FTZ into Singapore's customs territory for domestic consumption.

FTZ authorities are appointed to administer, maintain and operate FTZs, including ensuring the security of the premises within FTZs. FTZs are secured and fenced-up areas, with security contractors appointed by FTZ authorities to oversee the physical security of FTZs. All movement of goods between FTZs and Singapore's customs territory, as well as cross-border via land, must be accompanied by cargo clearance permits issued by Singapore Customs. The entry and exit points are manned by ICA and/or auxiliary police to control the physical movement of goods into and out of the FTZs and these goods may also be subjected to documentary checks and/or physical inspections at the checkpoints using a risk-based approach. Any discrepancies are referred to Singapore Customs or the relevant controlling agency for their follow-up investigation.

There are legal provisions to restrict the type of activities allowed to be performed inside FTZs, and failure to comply is an offence. Permissible activities include warehousing and minor re-packing or re-labelling, and retail operations are limited to those essential for the smooth operation of the FTZ (e.g. canteens for workers).

Singapore Customs also conducts periodic and surprise checks/audits on companies based inside FTZs to ensure their compliance with Singapore Customs' requirements. Certain movements of dutiable goods are further subjected to rigorous controls through the sealing of containers and customs supervision. There are multiple levels of controls to ensure high accountability of cargo movements.

Businesses which are located within FTZs are subjected to the same domestic AML/CFT laws and regulations. For example, they are mandated by law to report suspicious transactions to STRO. Singapore Customs also refers suspected ML cases to the CAD for follow-up investigation.

Physical Movement of Currency and Bearer Negotiable Instruments

In November 2007, Singapore implemented the cross-border cash movement reporting regime which requires persons to submit a cash movement report (CMR) when bringing into or taking out of Singapore more than $30,000 or equivalent in cash or bearer negotiable instruments (CBNIs). Anyone who fails to do so will be liable to an offence that carries a punishment of up to three years imprisonment and/or a fine of up to $50,000.

The CMRs enrich our financial intelligence database, and are used for detecting and preventing ML/TF and related crime. STRO provides CMR information both spontaneously and upon request to the relevant enforcement agencies, such as ICA, and the Cash Enforcement Branch, the unit within CAD responsible for the enforcement of the regime.

ICA, Singapore Customs and SPF work closely in the prevention of ML/TF through the cross-border movement of CBNIs. In cases where any CBNI is suspected to be linked to a crime, including ML/TF, police officers will investigate into these cases and seize the CBNIs. There are also detailed standard processes and procedures for investigators to follow to determine whether the undeclared or falsely-declared funds are linked to the commission of any domestic or foreign crime.

Overall

The combination of strong laws and tough enforcement of ML/TF activities serve as an effective deterrence to potential criminals and terrorists and help to ensure that Singapore's ML/TF risks emanating from our legal, judicial and institutional environment remain low. But as the threats associated with ML/TF are constantly evolving, periodic revision of the legal framework and re-calibration of our enforcement responses are required for Singapore to stay ahead and continue to meet international standards.

Prosecution and the Court System

The Attorney-General's Chambers (AGC) is an independent Organ of State. It is 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 (MLA) and extradition. It also provides legal advice to government departments and law enforcement agencies on the interpretation of AML/CFT laws and issues.

Based on investigations by enforcement agencies, the Public Prosecutor controls and directs all criminal prosecutions and proceedings in Singapore. This includes applying for a confiscation order against a defendant in respect of the benefits derived from criminal conduct if the court is satisfied that such benefits have been so derived.

The Economic Crimes and Governance Division[14] of AGC is primarily responsible for prosecutions and all related appeals in respect of white-collar and other commercial crimes, as well as corruption cases. This includes ML/TF offences as well as most of the serious offences listed in the CDSA.

It is important to have effective coordination between the enforcement and prosecution functions of the government, including reducing the gestation period between the commencement of investigations and the start of prosecutions. To this end, AGC has launched an initiative to station Deputy Public Prosecutors in several law enforcement agencies to provide immediate guidance to investigative officers, to improve the investigative qualities of cases and to generally expedite the investigation and subsequent timely prosecution or withdrawal of cases. This initiative is on top of the satellite office in CAD to provide legal advice and facilitate the disposition of cases.

The Subordinate Courts plays a key role in the administration of justice in Singapore. It has entrenched its commitment to meet the highest standards of integrity and efficiency and in doing so, serves the needs of the public with a service-centric ethos and commitment that permeates every aspect of its work. It has received numerous awards, with the most recent being the UN Public Service Award. The Subordinate Courts was also awarded the second prize in the category of "Improving the Delivery of Public Services" for Asia and the Pacific region for the establishment of its HELP[15] Centre. Domestically, it recently received the Public Service Premier Award for achievement of outstanding standards in organisational excellence in financial year 2011.

In order to improve judicial efficiency, the Criminal Justice Division, the largest division in the Subordinate Courts[16], set up a framework to facilitate the early resolution of criminal cases. The pilot phase of the Criminal Case Resolution (CCR) was launched at the end of 2009 and implemented formally in October 2011. The objective of the CCR is to assist in the resolution of criminal cases at an early stage through neutral facilitation by a senior Judge. In 2012 alone, more than 75% of the cases referred to CCR were resolved successfully, resulting in the savings of 120 hearing days. CCR ensures that the Subordinate Courts is able to identify cases which are likely to be resolved without proceeding to a hearing. This saves time for all parties involved and also ensures that precious hearing days are not wasted.

[14] The Economic Crimes and Governance Division was formed on 1 January 2011, demonstrating AGC's continuing commitment to enhancing our capability in dealing with increasingly complex financial and regulatory offences in today's globalised economy. The division, together with the State Prosecution Division and the Criminal Justice Division, form the Crime Cluster. Officers of the division also handle regulatory enforcement matters affecting the financial services sector, judicial review cases relating to criminal law proceedings and contempt of court cases. The division is organised into four specialised directorates, namely the Financial and Securities Offences Directorate, the Corruption Directorate, the General Commercial Crime Directorate and the Governance Directorate.

[15] HELP stands for "Helping to Empower Litigants-in-Person".

[16] The Subordinate Courts is made up of 5 Divisions, namely the Civil Justice Division, the Criminal Justice Division, the Family & Juvenile Justice Division, the Corporate & Court Services Division and the Strategic Planning Division.

The Criminal Justice Division is organised into seven specialised groups, each headed by a group manager. One of the groups is the Commercial Crimes Group, which is made up of nine Trial Courts specialising in criminal cases relating to commercial crimes, corruption, immigration, special drugs and intellectual property. Some of the judges from this group also participated in international conferences and exchanges such as speaking at the Regional Forum on "Corruption and Other Financial Crimes".

Overall, strong enforcement and prosecution cooperation, an efficient court system and specialisation in handling ML/TF commercial crime have helped to reinforce the effectiveness of the domestic institutional framework.

International Cooperation

Formal Cooperation

Singapore's Mutual Assistance in Criminal Matters Act (MACMA) permits the provision of a wide range of assistance without the need for a mutual legal assistance (MLA) treaty with Singapore so long as there is an undertaking of reciprocity. The details are available on AGC's website[17]. Singapore has clear and efficient processes in place for the execution of formal requests in a timely manner. There are established process flowcharts, standard operating procedures, timeline requirements and monitoring mechanisms for processing MLA requests.

Dual criminality is a well established requirement adopted by many jurisdictions in international cooperation and is recognised by FATF. In Singapore, the alleged criminal conduct is examined as a whole to determine whether the conduct would amount to a scheduled offence for which Singapore can provide assistance; it is not the label of the foreign offence or its constituent elements that must match a scheduled offence in Singapore.

Singapore also has an effective extradition regime. This was assessed to be fully compliant in respect of ML offences during our last FATF assessment in 2007/2008. Extradition of individuals charged with ML offences to and from declared Commonwealth countries and territories is possible in the absence of a separate extradition treaty. Extradition to non-Commonwealth countries is possible if there is a bilateral extradition treaty with the requesting country.

[17] Please refer to http://app.agc.gov.sg/What_We_Do/International_Affairs_Division/Mutual_Legal_Assistance.aspx

TF offences are also deemed extraditable crimes under the Extradition Act by virtue of Section 33(1) of the TSOFA. This applies to countries with which there is a formal extradition arrangement or treaty and all other countries that have ratified the International Convention for the Suppression of the Financing of Terrorism. Furthermore, Singapore can also extradite its own nationals as our Extradition Act does not distinguish based on nationality.

BOX ITEM 2C: CASE STUDIES ON MUTUAL LEGAL ASSISTANCE

Production of Bank Records

Singapore had assisted the United States (US) in its investigations into the three largest internet poker companies and their principals, focused on bank fraud, illegal gambling offences and the laundering of billions of illegal gambling proceeds. The companies, which operated major online gambling sites – PokerStars, Full Tilt Poker and Absolute Poker – were suspected of circumventing US laws on gambling-related payments by deceiving US banks into facilitating such transactions. It was believed that as a result, billions of dollars left the US each year for offshore internet gambling disguised as other types of financial transactions. Singapore's assistance, which included the production of bank records, assisted in the US investigations and eventually contributed to a successful resolution of the case: namely, a US$731 million settlement in relation to PokerStars and a US$50 million settlement in respect of its CEO, Mark Scheinberg.

Enforcement of a Foreign Confiscation Order

In 2009, acting on information received from Bangladesh and the US, Singapore commenced corruption investigations against a Singapore company. Investigations in Bangladesh and the US revealed that large amounts of funds were paid into the company's bank account in Singapore, and that these were bribes in relation to projects in Bangladesh for the development of a mobile telephone infrastructure and the building of a mooring container terminal.

In March 2011, Bangladesh and the US made a joint MLA request to Singapore to enforce a US confiscation order in connection to the company's account. Singapore acceded to this request, resulting in the return of US$2 million from the account to Bangladesh.

Creative Approach to Asset Recovery

In 2011, Bangladesh made an MLA request to Singapore to enforce a Bangladeshi confiscation order. This request was related to the joint request by the US and Bangladesh, but involved a different bank account belonging to another Singapore company. Even though the confiscation order could not be enforced in Singapore because it did not meet Singapore's statutory requirements, Singapore succeeded in returning almost US$1 million to Bangladesh by using a domestic court process designed for disposing property seized in the course of investigations.

Informal Cooperation

As Singapore's FIU, STRO is empowered under Section 41 of the CDSA to enter into MOUs with its counterparts to facilitate the exchange of information and financial intelligence in relation to MF/TF and other serious offences. STRO is also able to exchange information through the Egmont Group of FIUs[18], and has access to other forms of cooperation available to enforcement agencies such as the International Criminal Police Organisation (INTERPOL).

As a member of INTERPOL, SPF had shown Singapore's commitment to international and regional policing efforts by hosting events such as the 27th ASEAN Chiefs of Police Conference (2 - 7 June 2007), the 78th INTERPOL General Assembly (11 - 15 October 2009) and the 6th Pearls in Policing Conference (9 - 13 June 2012) in Singapore. SPF has also concluded MOUs with its strategic partners such as Australian Federal Police, Royal Brunei Police Force, Hong Kong Police Force and New York Police Department to enhance bilateral exchanges and joint cooperation in various fields.

CNB cooperates actively with foreign law enforcement agencies on a bilateral basis which involves the exchange of information and intelligence relating to drug trafficking and drug-related ML offences. CNB also works closely with international and regional drug law enforcement agencies such as the US Drug Enforcement Administration, the Australian Federal Police and the Narcotics Crime Investigation Department (Royal Malaysian Police).

At the informal level, CPIB cooperates with regional anti-graft agencies such as the Anti-Corruption Commission (Malaysia), Anti Corruption Bureau (Brunei Darussalam), Corruption Eradication Commission (Indonesia) and Independent Commission Against Corruption (Hong Kong) as well as the Federal Bureau of Investigation (US), Australian Federal Police and the Serious Fraud Office (UK) in the exchange of information, intelligence and joint operations. CPIB has assisted its counterparts in their requests for information except for information that can only be obtained through the use of coercive powers (for which countries may request through the MLA channel).

The Casino Regulatory Authority (CRA) has a well developed international network with its foreign counterparts and is often invited to attend key international fora and conferences where gaming regulators from around the world meet to exchange views, share information and foster stronger cooperation. Examples of such platforms include the Australasian Casino and Gaming Regulators' Conference, Gaming Regulators European Forum and the International Association of Gaming Regulators. In addition, CRA enjoys a high level of cooperation with counterparts in different regions and engages them through mutual visits where cooperation and information sharing agreements are made bilaterally.

As the integrated supervisor of financial services and financial stability surveillance, MAS has powers to obtain and exchange supervisory information in respect of regulated entities and groups. MAS is a signatory to numerous bilateral MOUs and also multilateral MOUs (MMOUs) such as the International Association of Insurance Supervisors MMOU and the International Organization of Securities Commissions MMOU. These arrangements strengthen MAS' ability to cooperate and exchange information with foreign supervisors as well as facilitate effective consolidated supervision of international FIs. Beyond responding to information requests on a timely basis, MAS also spontaneously shares information with other supervisors, such as pertinent concerns on an FI's ML/TF risk management controls and inspection reports.

[18] The Egmont Group of FIUs is an informal network of FIUs established for the stimulation of international cooperation. The Group meets regularly to find ways to promote the development of FIUs and to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

To facilitate cross-border supervisory cooperation, home country supervisors may conduct on-site examinations of the Singapore branch of an FI under its supervision to verify its compliance with the home country's AML/CFT policies and procedures. Home country supervisors may also choose to appoint auditors (both internal and external) of the bank's Head Office to conduct on-site examinations. In addition, MAS continues to organise and participate in supervisory colleges, including AML/CFT colleges, where key risks, concerns, and issues, including those related to ML/TF, are shared. The supervisory colleges also provide for effective communication and regulatory oversight between relevant supervisors.

Singapore currently engages in exchange of information for tax purposes in accordance with the internationally agreed Exchange of Information Standard (EOI Standard). The EOI Standard can be found in Article 26 of the 2005 model of the OECD Model Tax Convention or the 2002 OECD Model Tax Information Exchange Agreement (TIEA). Currently, EOI assistance may be extended to our partners via a bilateral agreement for the avoidance of double taxation which has been updated to contain the EOI Standard, or a tax information exchange agreement. On 14 May 2013, Singapore announced that EOI assistance will be extended to all existing tax agreement partners, without having to update each bilateral tax agreement individually. The Income Tax Act has since been amended to effect this. In addition, EOI assistance may be extended via the Convention on Mutual Administrative Assistance in Tax Matters, which was signed by Singapore on 29 May 2013. The legal provisions providing for EOI cooperation with our partners can be found in Section 105 of the Income Tax Act.

Singapore recognises that effective international cooperation is essential to the fight against ML/TF. Notwithstanding the strong level of informal cooperation and good working relationship between our agencies and their foreign counterparts, we are also considering how we can further enhance our international cooperation regime given the revised FATF Recommendation on other forms of international cooperation (R.40).

3. Prevailing Crime Types

Overview of ML/TF in Singapore

The assessment of Singapore's ML and TF threats is based on a detailed analysis of the indicators/factors that the relevant law enforcement agencies have identified to be relevant and unique to Singapore's context[19].

In general, the domestic crime rate[20] is relatively low in Singapore, largely due to the deterrent effect of stringent and effective law enforcement. This has helped to keep the ML threats arising from domestic crime generally low too.

However, as an international transport and financial centre with a significant foreign population, Singapore is exposed to the threats of ML arising from foreign predicate offences. Foreign predicate offences constitute 34% of all ML convictions between 2007 and 2011. The amount of foreign criminal proceeds seized amounted to $265 million. The main conduits of ML are banks, remittance agents, shell companies and individual money mules.

For the same reasons, and given Singapore's geographical neighbourhood, we may appear to be particularly susceptible to TF risks. However, there has been no evidence of TF being committed in Singapore or terrorist funds flowing into or through Singapore. There has also been little evidence of non-profit organisations (NPOs), charities and commercial entities in Singapore being exploited for terrorism-related activities. Since the Singapore Jemaah Islamiyah (JI) network was disrupted in 2001/2002, there has been no indication of any attempt by the JI to regroup in Singapore, or an emergence of another organised terrorist group in Singapore.

[19] The assessment of Singapore's domestic ML threats focussed on the most commonly committed predicate offences in Singapore. The indicators / factors analysed were divided into two groups ("determining factors" and "background factors") to differentiate their levels of impact on the ML threats. Based on the determining factors, relevant agencies were asked to provide preliminary assessments of the ML threat levels for the predicate offence(s) they were responsible for enforcing. CAD, being the lead agency for enforcing ML offences in Singapore, checked if the assessed threat levels were reasonable, taking into account background factors such as the number of ML cases investigated or prosecuted and the number of STRs filed. A similar approach was used to assess foreign ML threat levels.

For the TF threat assessment, the law enforcement agencies assessed the likelihood of TF activities occurring in Singapore or of Singapore being used as a conduit for TF funds. This assessment was based on investigations performed and intelligence / information received by the relevant agencies. This approach is similar to what is described above for the ML threat assessment. Indicators / factors were also grouped into two categories to differentiate their levels of impact on the TF threats.

For funds generated domestically, the propensity for suspected terrorists in Singapore (based on *modi operandi* and tell-tale traits / behaviour of terrorists) to raise funds locally for acts of terrorism either at home or abroad was considered. For funds generated overseas, the likelihood of overseas-based terrorists using Singapore as a conduit for TF purposes or suspected terrorists in Singapore using foreign sources of funds to support their activities locally was considered. The number of incoming and outgoing requests for information pertaining to suspected TF cases in Singapore was also taken into account. The assessment made based on the approach above was then cross-checked against other background factors.

[20] In its 2010 Global ML and TF Threat Assessment, the FATF noted that white-collar financial crimes of a predominantly global nature were increasingly becoming a primary source of laundered money and that criminals were maximising the opportunities presented by new technologies to conduct these illicit activities. As an international financial centre, Singapore remains vigilant against illicit flows of funds. Law enforcement agencies also work closely with the financial sector to fortify the lines of defence against abuse by criminals. Domestically, the commercial crime situation remains under control. From 2007 to 2011, the average commercial crime rate ranged from 67 to 78 per 100,000 of the population. There was a slight increase in the number of commercial crimes in 2011 mainly due to incrementally more cheating and related offences. However, the authorities have taken swift action to tackle this increase, including intensifying efforts to educate the public on how to identify and avoid the latest scams. SPF also works closely with banks and MAS to enhance the security of payment card systems.

ML Threats – Domestic Origin

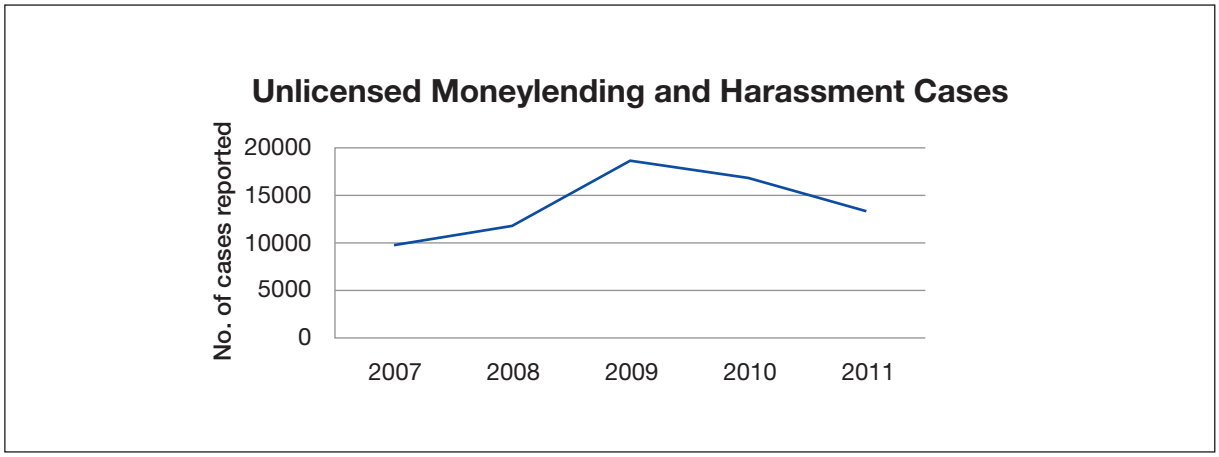
Of the common predicate offences committed in Singapore[21], unlicensed moneylending (UML), cheating and criminal breach of trust (CBT) are identified as the major ML threats that all relevant stakeholders concerned with AML matters should pay attention to.

Unlicensed Moneylending

In Singapore, anyone conducting a moneylending business is required to obtain a licence from the Registry of Moneylenders. Loansharks, or "Ah Longs" as they are commonly known in Singapore, are unlicensed moneylenders that typically exhibit the following undesirable characteristics:

- Charge exorbitant interest rates on loans;
- Impose dire consequences for default/late payments; and
- Use aggressive harassment tactics against defaulters and innocent parties.

The following chart shows the total number of UML and harassment cases reported yearly from 2007 to 2011. Harassment cases accounted for more than 90% of the total number of cases reported. There was an increase in the total number of cases until 2009. Since then, the number of cases reported has declined steadily, owing to the authorities' robust enforcement efforts in cracking down on UML and harassment activities amid concerns over negative social externalities.



[21] A list of the commonly occurring predicate offences in Singapore was examined. The list comprises offences such as cheating, corruption, CBT, drug trafficking, forgery, illegal gambling, immigration offences, misappropriation, robbery, theft, UML and vice.

During the launch of the inaugural Anti-UML Public Education and Awareness Campaign on 30 November 2012, Deputy Prime Minister Teo Chee Hean said, "UML is a criminal activity. It does not just affect the borrower, but also the borrower's family and his or her neighbours. The harassment tactics used by loanshark syndicates such as locking gates, spraying paint on walls and doors, and even starting fires in corridors, create alarm in the neighbourhood, cause inconvenience and pose danger to innocent people. Such tactics strike fear among Singaporeans, in what should be the safe sanctuary of their homes and neighbourhood."

Unlicensed Moneylending and ML

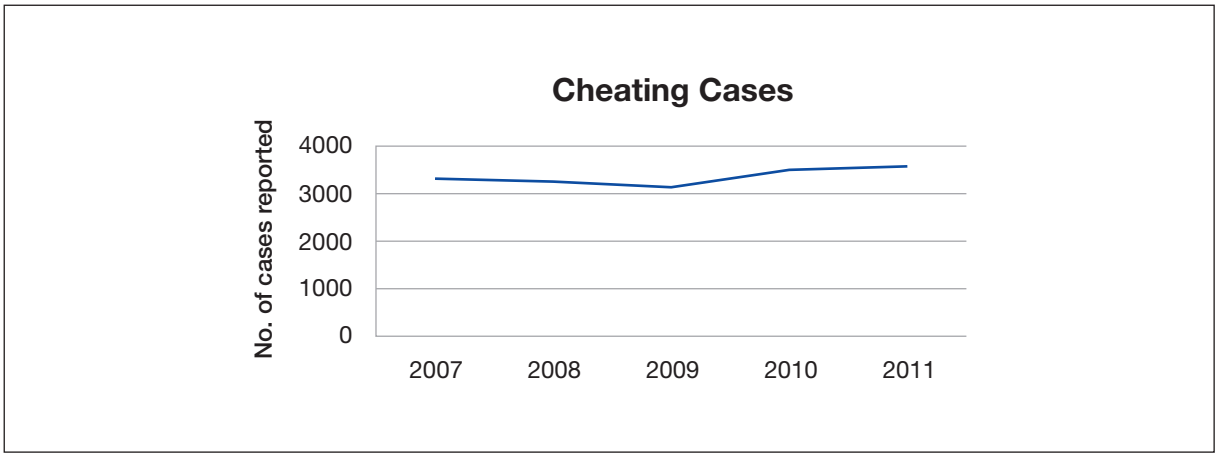
UML syndicates often lend money at exorbitant interest rates ranging from 20% to as high as 1000% per annum, typically to desperate people who have incurred more expenses or debts than they could service and are unable to obtain loans from legitimate sources. The sizes of loans offered by UML syndicates to their debtors are generally small (ranging from $500 to $1,000) to minimise loan default risk[22]. However, with the high interest rates, syndicates can generate sizeable criminal proceeds.

Given the cash-intensive nature of UML activities, bank accounts are often used to facilitate fund transfers of UML syndicates. These bank accounts often belong to individual money mules, who are usually either debtors who surrender their bank accounts to the UML syndicates due to the inability to pay their debts or individuals who sell their bank accounts in order to earn commission. Loans are disbursed and repaid using the mules' bank accounts via multiple cash deposits from various debtors and cash withdrawals on an almost daily basis[23].

UML is one of the most prevalent ML predicate offences in Singapore. The authorities have rigorously pursued all cases involving UML and the related offence of ML. While the amounts involved in UML are not always large, its prevalence has a significant adverse impact on the social well-being of the general population. It also creates a negative influence on youths as they are recruited to carry out harassment activities by being promised "easy money". SPF has arrested offenders as young as 15 years old. There are also additional costs involved in rectifying the damage caused by harassment such as vandalism.

Cheating

There has been a slight increase in the number of cases involving cheating and related offences[24] reported in recent years, as seen in the following chart:



[22] This is based on the law enforcement agencies' strategic analysis of financial intelligence.

[23] This is based on the law enforcement agencies' strategic analysis of financial intelligence.

[24] Cheating is an offence under Sections 417 and 420 of the Penal Code. Simple cheating is punishable under Section 417 with an imprisonment term of up to a year, a fine or both. Aggravated cheating is punishable under Section 420, with an imprisonment term of up to seven years, a fine or both.

In particular, SPF has observed a rising trend in cheating and related offences using the following *modi operandi*:

(i) *Failure to Deliver Goods and Services*

These cases mainly involve victims who make purchases in response to fraudulent advertisements (often on the internet) but subsequently fail to receive the goods or services paid for. Examples include holiday packages, car rentals and hotel accommodation which are attractively priced to lure unsuspecting victims. Another notable trend is that most of these failure to deliver goods and services cases usually involve multiple victims due to the use of mass media.

(ii) *Inducement of Victims to Purchase Counterfeit Goods*

In these cases, the perpetrators would sell items such as gold, luxury watches and electronic products to victims on the premise that they are authentic, when they are in fact counterfeits.

(iii) *Continued Prevalence of Kidnap Phone, Lottery Phone and Internet Love Scams*

Kidnap Phone Scams

The kidnap phone scam first surfaced in August 2007. Generally, culprits would call the victims and claim that their family members have been kidnapped. The "kidnappers" would then demand the victims to transfer a sum of money as ransom to various local and overseas bank accounts.

Lottery Phone Scams

In these cases, the culprits would usually make unsolicited calls or send mobile text messages claiming that the recipients have won prize money in an overseas lottery. The recipients would then be directed to liaise with the lottery's agent or representative. Sometimes, recipients would be asked to provide their personal particulars and bank account numbers to facilitate the transfer of the prize money.

In truth, the victims have not won any lottery at all. The lottery scam is designed to dupe victims into parting with their money. After deceiving the victims into believing that they have won the lottery, the culprits would persuade the victims to pay a tax or other forms of administrative payments to secure the release of the "prize money". The culprits would abscond after receiving the money or conjure up more excuses to induce further payments from their victims.

Internet Love Scam

The internet love scam started becoming more prevalent in 2008. Typically, the culprits would befriend victims through online dating or social networking sites. The culprits, believed to be foreigners, would develop rapport or even a "love relationship" with their victims, sometimes over a prolonged period of time, before making their move.

In some cases, the culprit would claim to be coming to Singapore to seek the victim's hand in marriage but would later claim to be detained at customs and in need of money to be released. In another variation, the culprit would claim to have mailed a gift to the victim but would request the victim to pay a fee to secure the release of the gift detained at customs. In yet another permutation, the culprit would request a loan from the victim due to financial difficulties, ask the victim to invest in a venture or invite the victim to be a director in a company.

In other cases, the culprits would request the victims to perform sexual acts over the internet and record photos or videos of these acts without the victims' knowledge. The culprits would subsequently threaten to circulate these compromising photos or videos and extort money from the victims. In all these cases, the culprits would cease all contact with the victims once the requested money is transferred to the designated overseas bank accounts.

Most of the cases target mass victims and the amount of loss per victim is relatively low. However, major cheating cases involving significant amounts of losses which may not fall into the typical *modi operandi* described above, have also been detected. An example of this is found in Annex A: ML Domestic Threats – Case Study on Cheating.

Cheating and ML

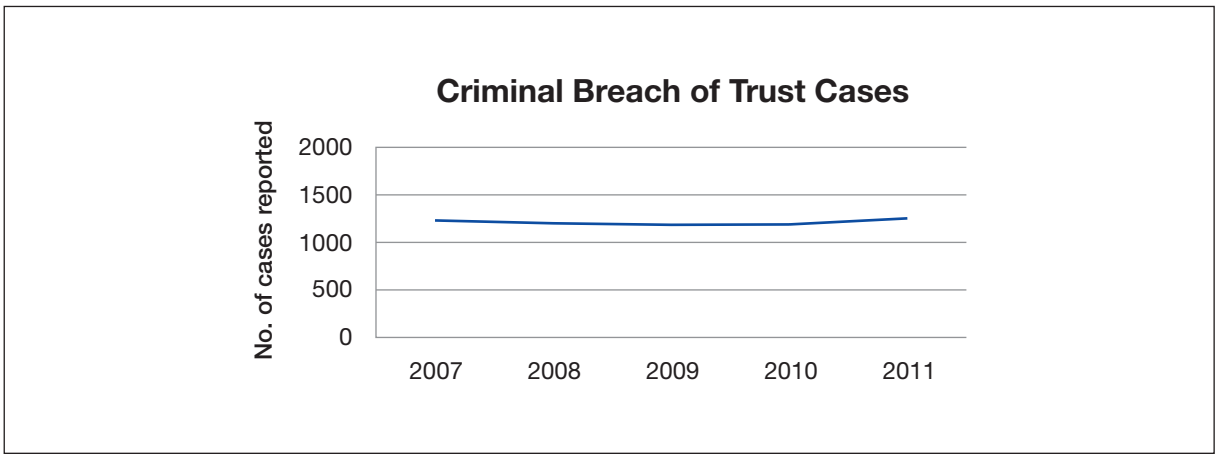
Cheating is one of the most prevalent ML predicate offences in Singapore. Due to its relatively higher incidence[25], it generated the highest amount of criminal proceeds among all predicate offences. The harm to society from cheating offences is often underestimated, particularly when we consider the aggregate impact on vulnerable victims such as the elderly. The large number of victims and ever-changing type of scams also require authorities to commit significant resources to enforcement and public education.

With the exception of kidnap phone, lottery phone and internet love scam cases, most of the other cheating cases involve lone operators rather than syndicates.

The culprits in kidnap phone and lottery phone scam cases rely heavily on the use of third-party or nominee bank accounts for the laundering of proceeds. As for other cheating cases, the proceeds are usually self-laundered. Common self-laundering methods include the transferring of illicit proceeds between several personal bank accounts and conversion of illicit proceeds into other realisable assets such as investments and properties.

Criminal Breach of Trust

The number of CBT[26] cases reported has remained relatively constant over the past few years, as shown in the following chart:



[25] As compared to the other commonly occurring predicate offences.

[26] Section 405 of the Penal Code defines CBT as "whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or diposes of that property, in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person to do so, commits CBT."

Under Section 406 of the Penal Code, a CBT offence is punishable with imprisonment of three years, a fine or both. Aggravated forms of CBT are provided for in Sections 407 to 409 of the Penal Code and these offences are punishable with more severe sanctions. These offences include CBT by carriers, clerks, servants, public servants, merchants, bankers and agents.

There is no clear pattern with respect to the amount of funds involved and the profile of the culprits. An example of a major CBT case handled by SPF can be found in Annex A: ML Domestic Threats – Case Study on CBT.

Criminal Breach of Trust and ML

While CBT is not as prevalent as cheating, the total criminal proceeds involved are significant. While most cases involve small amounts of losses, cases involving larger amounts are of particular concern. These are typically perpetrated by offenders who have been entrusted with key responsibilities and empowered to make financial decisions in their positions. These offenders abuse their positions and powers to benefit themselves such as to finance their personal gambling habits or feed their greed.

Offenders who commit CBT tend to be well-educated and as such, are able to exploit a wide variety of ML methods, though the preferred ML conduit is still the banking system. A review of the offenders' bank accounts would usually reveal transactions that are not commensurate with their financial means. Offenders also typically operate alone, so almost all CBT cases involve self-laundering of illicit proceeds.

The actions of these offenders result in great financial losses for both public and private institutions and damage the public's trust in these institutions.

Other Criminal Threats of Interest – Domestic Origin

Besides UML, cheating and CBT, the table below contains information about other criminal threats of interest:

Criminal Threat	Nature and Extent	Method of ML
Corruption	Corruption in Singapore remains low and under control, with no significant increase in the number of complaints and cases investigated over the past five years. Nonetheless, the majority of corruption cases (more than 80%) involve money as gratification and hence, criminal proceeds are generated at a moderately high level. The average amount of criminal proceeds involved per case is one of the highest out of all the different types of crimes.	According to many international reports, when a person accused of corruption is a politically exposed person (PEP), the possibility of ML is very high. While Singapore recognises this possibility, the number of domestic corruption cases involving domestic PEPs is low. In 2011, there were no such cases. Based on investigation findings from domestic corruption cases, the offenders do not usually deposit the funds in their own bank accounts if the proceeds are substantial. They instead park their funds with trusted third parties and also use the proceeds from corruption to buy high-value items such as properties and motor vehicles. There have not been cases of criminal proceeds from domestic corruption being laundered via international fund transfers.

Forgery	The incidence of this offence is relatively low though the offence could potentially generate significant amounts of criminal proceeds. The average amount of criminal proceeds involved per case is moderate. The offence may be one-off or be part of a series of offences committed over a number of years. The most common form of forgery, which involves the highest quantum of criminal proceeds, is the forging of signatures on financial instruments such as cheques.	This offence is usually committed by individuals. Criminal proceeds from forgery are typically self-laundered via the banking system.
Vice[27]	The incidence of this offence is relatively low. The total quantum of criminal proceeds involved in all vice investigations in 2011 was moderate.	The cases detected were committed mostly by individuals or small groups of individuals. The amount of criminal proceeds generally ranges from moderate to large. The criminal proceeds are seldom converted into other forms and are mainly used for personal consumption. For some of the vice cases, law enforcement agencies seized cash.

[27] Vice activities included in this risk assessment are:
(i) Bringing women into Singapore for the purpose of prostitution (Section 140(1)(d) of the Women's Charter)
(ii) Living on the earnings of a prostitute (Section 146 of the Women's Charter)
(iii) Managing a place of assignation (Section 147 of the Women's Charter)

Offences under Sections 140, 146 and 147 of the Women's Charter are punishable with up to five years' imprisonment, a fine or both. In the case of a second or consequent conviction under Section 147 of the Women's Charter, the offence is punishable with up to 10 years' imprisonment, a fine or both.

Illegal Gambling and Related Offences[28]	The incidence of the offence ranges from low to moderate. The total quantum of criminal proceeds involved in all illegal gambling investigations in 2011 was moderate, and the average amount of cash seized per case was low for common gambling activities whereas, the average amount per case involving a bookmaker was moderate.	Illegal gamblers are mostly individuals or small groups of individuals, with the crime committed generally being opportunistic in nature. The amount of criminal proceeds is generally small for common gambling offences. The criminal proceeds are seldom converted into other forms and mainly used for personal consumption. For some illegal bookmaking cases, law enforcement agencies seized cash which was generated from the collection of illegal bets.

[28] Illegal gambling activities included in this risk assessment are:
(i) Owner / occupier of premise used as common gaming house (Section 4(1) of the Common Gaming Houses Act)
(ii) Managing a common gaming house (Section 4(1)(c) of the Common Gaming Houses Act)
(iii) Assisting in public lottery (Section 5(a) of the Common Gaming Houses Act)
(iv) Gaming in public (Section 8(2) of the Common Gaming Houses Act)
(v) Acting as a bookmaker (Section 5(3)(a) of the Betting Act)

Offences under Section 4 of the Common Gaming Houses Act are punishable with up to three years' imprisonment, a fine or both. Offences under Sections 5 and 8 of the Common Gaming Houses Act are punishable with up to five years' imprisonment, a fine or both. Offences under Section 5 of the Betting Act are punishable with up to five years' imprisonment, a fine or both.

To strengthen our efforts against illegal gambling, the authorities are currently studying a proposal to introduce new laws to give our law enforcement agencies the powers to act against facilitators and providers of, and intermediaries involved in remote gambling services. The authorities are also considering introducing measures to block access to gambling websites and payments to remote gambling operators, and to prohibit advertisements promoting remote gambling.

TF Threats – Domestic Funding

As a financial and transportation hub, Singapore is vulnerable to terrorist elements seeking to exploit our hub status to raise funds domestically for terrorism-related activities. Our geographical location and the presence of a significant foreign community further expose Singapore to the threats of TF.

Law enforcement authorities spare no effort to detect and investigate every possible TF lead. Notwithstanding these efforts, there has been no evidence of TF being committed in Singapore or of funds being raised domestically for terrorism-related activities here or abroad.

The robust CT and CFT measures that Singapore has put in place provide strong safeguards against the threat of funds being generated domestically through illegitimate and criminal means for terrorism purposes. While Singapore has detected several self-radicalised individuals since 2007, none contemplated mounting attacks in Singapore. They had instead been intent on making their way to theatres of jihad overseas to become militant jihadists. Nonetheless, authorities are mindful that there remains the possibility that self-radicalised individuals may donate funds to support overseas terrorist groups.

There have been academic reports stating that terrorist groups in the region used indigenous methods to fund their activities. Some have resorted to using criminal means like robbery to finance their operations, while others were reportedly increasingly relying on drug trafficking and the hacking of online accounts to fund their activities. It has been speculated that these groups resorted to crime because of difficulties faced in raising donations and obtaining international funding amid continuing counter-terrorism operations against these groups.

Terrorist and criminal elements have also been quick to exploit new payment technologies and other emerging trends like phone and internet banking to carry out fraud and other illicit activities and covertly move funds. New payment technologies such as mobile payment technology have enabled fund transfers to be made anywhere, anytime and by anyone with a mobile phone. These provide opportunities for financial transactions to be executed easily without the involvement of bank accounts or traditional payment methods. Singapore's laws are equipped to deal with such offences that involve the use of mobile or digital instruments, or the conduct of digital activities for TF purposes.

BOX ITEM 3A: THE TERRORISM THREAT IN SINGAPORE

Although the Singapore JI network has been disrupted following sustained security operations since 2001, Singapore continues to be a potential target for terrorist elements in the region. The JI-related terrorist elements remain active in new networks and organisations in Indonesia. In 2012, Indonesian police disrupted several plots in the country that targeted tourists and foreign diplomatic missions, among others. These plots, aimed at foreign entities, indicate that terrorist elements retain an interest in targeting perceived "enemies" beyond Indonesia and its authorities. These developments are of concern given that Singapore remains on the radar of regional terrorist elements.

At the same time, Singapore remains vigilant against Hizbollah and Iranian elements in the region, as seen from the foiled plans in Thailand in January and February 2012, which have added to the terrorism threat faced by Singapore. Notably, Hizbollah elements had previously plotted attacks in this region, which included Singapore.

At the global level, Al-Qaeda and its affiliates have suffered significant setbacks, including the loss of key leaders and operatives in recent years. However, Al-Qaeda and its affiliates have exploited the instability in parts of the Middle East and North Africa in the aftermath of the Arab Spring to expand their operations and establish safe havens in places including Yemen, Sinai in Egypt and Mali, where they can train recruits for local and external attacks.

The Al-Qaeda core continues to provide ideological justifications for jihadi terrorism and has promoted the idea of individually planned and executed attacks unaided by any larger terrorist organisation in recent years. The internet has been exploited to this end and Singapore, like many other open and globalised societies, has not been spared from the threat of self-radicalisation. Between 2007 and 2013, ISD detained five self-radicalised Singaporeans. They were not members of any organised terrorist group but had been inspired and radicalised by Al-Qaeda's global jihadist ideology through what they had read on the internet. None had contemplated mounting attacks in Singapore; they were instead intent on making their way to theatres of jihad overseas to become militant jihadists.

The terrorism landscape has undergone significant changes since 2001 but the threat of terrorism persists, both globally and in the region. The Singapore Government will continue to take preventive and defensive measures to safeguard the security of Singapore and contribute towards international efforts to fight terrorism.

The Funding of JI Network in Singapore

Investigations into the local JI revealed that it was largely self-financed by members who contributed 5% of their monthly salaries. The monthly contributions were collected by the treasurer of each JI cell and then handed over to the overall treasurer of the Singapore JI network. The overall treasurer kept the money in his home and maintained the accounts. Half of the collections of the Singapore JI network were channelled to the JI leadership in Malaysia and in turn, disbursed to the Indonesian and Malaysian JI networks equally and delivered by hand using trusted couriers. The remaining funds were used to finance the Singapore JI network's local activities, as well as to render financial assistance to members who were less well-off.

Investigations also revealed that the Singapore JI members eschewed the commercial banking system, primarily because these commercial institutions were interest-generating and hence regarded as haram (that is, forbidden). Most, if not all, of the JI members had little funds in their bank accounts, and investigations into and detailed financial profiling of the account transactions revealed that the accounts were not used for terrorism purposes.

Some Singapore JI members had their own businesses and were encouraged to contribute 10% of their earnings to the JI network as well. There were no indications, however, that charities or other NPOs in Singapore were used by the JI network to raise funds for terrorism purposes.

Since the disruption of the Singapore JI network in 2001, these financing activities have ceased.

ML Threats – Foreign Origin[29]

ML, cheating and corruption have been identified as predicate offences of foreign origin which pose relatively higher ML threats to Singapore. This assessment was based on the incidence of cases, details of the relevant predicate offence, ML investigation units, and international typology reports.

ML and Cheating

ML is most typically cited as one of the offences being investigated by foreign law enforcement agencies in their requests to Singapore for assistance. Of particular concern is the spike in the number of ML cases involving shell companies.

Shell Companies

Shell companies are registered in Singapore or elsewhere with no legitimate business activities and minimal paid-up capital. The authorised bank signatories are foreigners based overseas who are usually the companies' directors and shareholders. For companies registered in Singapore, the resident director[30] would usually be a nominee who has no access to the bank accounts and holds no shares in the companies. In most cases, the foreign directors employ the services of a corporate service provider (CSP). Some CSPs provide multiple services from incorporating a company, facilitating the opening of bank accounts in Singapore, and providing a Singapore-registered address and a nominee resident director. These CSPs can earn an annual income of approximately $3,500 to $6,000 per company for these services.

There have been instances where suspicious activities, such as frequent and large incoming remittances from different overseas individuals and companies, were observed after the Singapore bank accounts were opened. Following the receipt of funds in the Singapore bank accounts, the funds were remitted out of Singapore within the next few days.

It would later be discovered that these were remittances of criminal proceeds from overseas. The predicate offence was typically cheating, which took various forms ranging from investment scams to hacking of email accounts. An example can be found in Annex A: ML Foreign Threats – Case Study on Cheating Involving a Shell Company.

The risks of ML via a shell company's bank accounts, if not mitigated effectively, can affect the reputation of our financial sector. CAD has conducted consultation sessions with the regulators to discuss strategies to combat this threat.

CAD has developed standard operating procedures for the detection and investigation of such cases. As these cases are linked to foreign predicate offences, CAD has also engaged its foreign counterparts to pursue the cases.

ML and Corruption

Law enforcement authorities have received several foreign requests for assistance in cases that involve the predicate offence of corruption. It is observed that the ML methods employed in such cases are either self-laundering via the banking system or third-party laundering via bank accounts of the suspect's family and close associates.

[29] The threat analysis of foreign origin is divided into two sections: crime-type analysis and jurisdiction analysis. The results of the latter are not available in this report, but will be disseminated to the private sector via other channels.

[30] Section 145 of the Companies Act requires that every company shall have at least one director who is ordinarily resident in Singapore.

In assessing the ML threats relating to overseas corruption, the 2008 FATF mutual evaluation report on Singapore was factored in – the report highlighted that significant ML risks associated with criminal proceeds generated in the region existed. FATF was of the view that Singapore's position as a stable and prominent financial centre in Southeast Asia increased its attractiveness as a destination for criminals to launder their criminal proceeds.

Overall, we recognise that ML threats of foreign origin, if not mitigated effectively, can impact international perceptions of our country's ML risks.

Other ML Threats of Interest – Foreign Origin

Match-Fixing

Match-fixing may involve acts of corruption to arrange the outcomes of sports games. Match-fixing activities are usually syndicated and transnational, given the global popularity of sports and the lucrative nature of the crime. Accordingly, besides corruption, match-fixing could also contain elements of conspiracy, betting fraud and ML. Law enforcement agencies have maintained strict vigilance over suspected football match-fixing activities and have taken action against the culprits. In the last 10 years, CPIB investigated 10 cases involving alleged football-related corruption in Singapore under the PCA. Six cases resulted in convictions. Stern warnings were issued in three other cases. SPF also takes firm action against illegal football betting. Over the last three years, SPF arrested an average of 56 persons each year for illegal football betting.

There are stiff penalties for corruption offences. Under Sections 5 and 6 of the PCA, persons convicted of corruption face fines not exceeding $100,000, imprisonment for up to five years, or both. In addition, under Section 13 of the PCA, persons who accept gratification may receive a financial penalty equivalent to the amount of gratification accepted. Any ill-gotten gains can also be confiscated under the CDSA.

Close cooperation between countries and law enforcement agencies is needed to effectively detect and combat match-fixing. For the recent global match-fixing syndicate case involving Singaporeans, SPF and CPIB established a joint investigation team to work with INTERPOL's Match-Fixing Task Force to pursue leads. The team obtained useful information from INTERPOL, the European Police Force (Europol) and European countries affected by the syndicate's match-fixing activities. This culminated in the island-wide arrest of 14 suspects in September 2013.

SPF and CPIB also work closely with the Football Association of Singapore (FAS) to ensure that the football scene in Singapore remains clean. Regular outreach efforts are carried out to educate players on the ills of corruption and its consequences. In addition, the agencies assist FAS in administering random polygraph tests on both Lions XII and S-League players. Any indication of suspicious match-fixing activities is reported and dealt with.

Other Criminal Threats of Interest – Foreign Origin

The following table contains information about other foreign criminal threats of interest:

Criminal Threat	Nature and Extent	Method of ML
CBT	The incidence of the offence is relatively low but there is a significant amount of criminal proceeds generated in each case.	Common ML methods employed by offenders include converting criminal proceeds into realisable assets such as investments and properties, and third-party laundering via bank accounts of the suspect's family and close associates.
Securities Market Misconduct	Securities market misconduct is one of the offences[31] cited in a couple of cases involving foreign jurisdictions.	Common ML methods include self-laundering via the banking system and laundering through remittances to or deposits into the bank accounts of the suspect or the suspect's company.
Drug Trafficking, Immigration Offences, Tax Offences, Trade-Based ML	It is noted that there are reports internationally that have cited these crime types as risk areas for Singapore but the number of cases investigated, foreign requests for assistance received and seizures relating to these offences is very low.	The reports did not state specifically the ML methods. For drug trafficking, the law enforcement experience is that drug traffickers in Singapore are low-level runners or couriers and payments received are of low value. Traffickers have limited impetus to launder their drug proceeds as the amounts of funds they deal with are small to start with. More often than not, the traffickers are drug abusers themselves and the proceeds from the trafficking go towards feeding their drug addiction.

[31] Possible securities market misconduct offences detected include dealing in securities without a capital markets services licence, market manipulation and unauthorised share trading.

Emerging ML Threat: Money Mules Recruited via Social Networking Websites

In 2012, SPF detected several cases in which foreign banks requested the recall of funds shortly after remitting them to bank accounts in Singapore. The requests claimed that the funds were transferred fraudulently.

Investigations by law enforcement agencies revealed that in many of these cases, the victims' email accounts were allegedly compromised, by a criminal syndicate, which used these accounts to send unauthorised instructions to the victims' banks to transfer funds to bank accounts in Singapore.

The bank accounts in Singapore were held by "money mules" who had been recruited by the syndicate via social networking websites to receive, withdraw or transfer funds. 159 money mules were identified in 2012. These money mules were often instructed by the syndicate to transfer funds to other syndicate members located overseas, and one of the popular modes of such transfers was via licensed remittance agents.

A total of about $24.6 million had been fraudulently transferred from bank accounts of overseas victims to money mules in Singapore. Funds would typically be remitted to the money mules' bank accounts and withdrawn or transferred immediately thereafter. However, proactive engagement of our foreign counterparts and swift action enabled our investigators to seize around 11% of the fraudulently -transferred funds.

The crime was orchestrated such that the funds flowed across several jurisdictions. This heightened the challenges faced by law enforcement agencies in each jurisdiction in their investigations. Due to the nature of the crime, it was imperative that law enforcement agencies from the various jurisdictions worked closely together to effectively tackle this spate of crimes.

Singapore has been proactively engaging the FIUs and law enforcement agencies of jurisdictions affected by this emerging ML trend. We have spontaneously exchanged financial intelligence information with our counterparts and shared our analytical report on this trend. Such cooperation has already resulted in several successful convictions in Singapore for various offences including ML. An example can be found in Annex A: ML Foreign Threats – Case Study on Money Mules.

The threat of ML via bank accounts of money mules, if not mitigated effectively, can affect the reputation of our financial sector. CAD has developed standard operating procedures on the detection and investigation of such cases. As these cases are linked to foreign predicate offences, CAD has been engaging our foreign counterparts to pursue the cases.

CAD has raised public awareness of the negative consequences of being an illegal money mule by distributing pamphlets at major banks and remittance agents, and issuing crime advisories via various media platforms including websites, newspapers and television programmes.

TF Threats – Foreign Funding

Singapore remains vulnerable to terrorism-related developments at the global and regional levels, and the possibility that terrorist elements may seek to direct funds from abroad to support terrorism activities in Singapore or use Singapore as a conduit for foreign TF cannot be discounted. As such, Singapore must continue to be vigilant against any attempts to channel funds into Singapore for terrorist activities, or use Singapore as a conduit for foreign TF.

To date, there is little evidence of foreign funds flowing into Singapore for terrorist activities, and of Singapore being used as a conduit for TF. That said, groups such as Al-Qaeda, Hamas and Hizbollah are known to have misused charities and other NPOs to raise funds. For instance, charities such as the Benevolence International Foundation, Global Relief Foundation and Holy Land Foundation for Relief and Development have allegedly provided financial and other assistance to Al-Qaeda or Hamas in the guise of charitable relief[32].

Separately, there are also concerns that terrorist elements are continuing to use the international banking and financial network to launder illicit funds for terrorism-related purposes[33].

In view of these external developments, Singapore has continued to maintain its vigilance and actively follows up on all leads relating to suspected TF going through Singapore.

[32] Between November 2001 and March 2008, there were 26 cases in the US which involved charges against charities or individuals associated with charities in relation to the provision of financial or material support to terrorist organisations. These trends are of concern to Singapore as they increase the likelihood of TF activities occurring here.

[33] The Hizbollah has reportedly deepened its foothold in the narcotics trade through criminal elements in the Lebanese émigré communities in South America. Closer to home, there have also been reports of the use of the financial system and other facilities to support terrorism-related activities. In November 2011, the Philippine National Police and the US Federal Bureau of Investigation reportedly arrested four persons in Manila over a hacking operation which targeted customers of the US telecommunications giant AT&T to funnel money to an unidentified Saudi-based terrorist group. According to media reports, the suspects remotely gained access to the telephone operating systems of an unspecified number of AT&T clients and used them to call telephone numbers which passed on revenue to the suspects. The Philippine National Police reportedly stated that the scheme, known as "remote toll fraud", resulted in almost US$2 million in losses incurred by AT&T. *Sources: "Manila, FBI arrest hackers who sent money to militants", Today, 28 November 2011; "Terror funds: 4 held in Manila over phone hacking", The Straits Times, 28 November 2011; and "Hacking against AT&T said to fund terror group", International Herald Tribune, 28 November 2011.*

Law Enforcement / Policy / Legal Responses

ML

The following table highlights the mitigating measures used to combat ML threats:

Strategy	Action Plan to Combat Threats of Domestic Origin	Action Plan to Combat Threats of Foreign Origin
1. Allocate sufficient law enforcement resources to priority areas	• Increase law enforcement resources to investigate ML arising from major crime threats.	• Increase law enforcement resources to investigate ML arising from major crime threats.
2. Investigate major crimes rigorously	• Formalise and update internal standard operating procedures to enhance the early detection, tracking and referral of possible ML offences. • Provide more guidance and training to law enforcement agencies on handling ML investigations.	• Implement policies such that whenever a request for international cooperation is received, the case is reviewed to determine whether there is a possibility that the funds generated from the crime were laundered in Singapore and if so, a ML case should be opened in Singapore. This review is to be conducted regardless of whether the foreign request involves ML. • Formalise and update internal standard operating procedures to enhance the early detection, tracking and referral of ML offences.
3. Strengthen cooperation between law enforcement agencies and their foreign counterparts	• Hold meetings between policy makers, regulators, law enforcement agencies and the FIU to explore new strategies in combating crime. • Continue to leverage on the financial intelligence provided by the FIU to detect crime.	• Review international cooperation and legislative framework in order to comply with revised FATF requirements. • Engage foreign counterparts. • Establish good relationships with foreign counterparts and understand each jurisdiction's ML vulnerabilities. • Continue to leverage on the financial intelligence provided by the FIU to detect crime.

4. Engage industry and community	Industry • Disseminate crime indicators to the various industries so that they would be able to detect and report suspicious transactions. • Collaborate with industry associations to raise awareness of major crimes.	Community • Educate the public so that they would not be used as money mules. • Conduct community engagement programmes via digital and traditional media platforms to raise awareness of major crimes to prevent more people from becoming victims.	• Disseminate crime indicators to the various industries so that they would be able to detect and report suspicious transactions. • Educate the public about the dangers of being used as money mules.

TF

Singapore has taken concrete steps to enhance our legislative framework and will continue to fine-tune it to ensure effectiveness in the face of the evolving ML/TF threats.

We will continue to strengthen upstream preventive measures. The Government alone is not able to tackle every security threat, and it recognises that people are key in fighting terrorism. Ensuring public vigilance is a continuing effort of the Government. We will continue to work closely with our community leaders to nurture bonds of trust with the community and to prevent terrorist ideology from infesting our community.

We will also continue to emphasise the building of stronger and closer partnerships with relevant industry groups through regular outreach programmes.

We will dedicate sufficient resources to look into this important area of work. Law enforcement agencies will also continue to work closely with STRO to detect and analyse suspicious transactions relating to TF.

4. Financial Sector Risk Assessment

Full Banks and Qualifying Full Banks

Introduction

Full banks[34] and qualifying full banks (QFBs) are licensed under and governed by the Banking Act. These banks may enter into the full range of banking businesses, including taking deposits, providing cheque services, lending and any other business that is regulated or authorised by MAS, such as private banking, insurance broking and capital market services. They are, however, prohibited from engaging in non-financial activities. Foreign full banks are typically allowed to operate from only one service location, while those with QFB privileges may operate from a total of 25 service locations (including automated teller machines). There is no location restriction for local full banks. At the end of 2012, there were six local full banks and 27 foreign full banks operating in Singapore, including 10 QFBs, with assets totalling $1.3 trillion.

ML Risks

Full banks and QFBs play a significant role in the financial sector and serve a broad spectrum of corporate and individual customers, which include higher-risk customers such as PEPs. These banks also offer high-value private banking facilities, which is a risk factor for ML.

These banks offer a wide range of products and services, including some cash-based products such as over-the-counter cash deposits and withdrawal services. The higher frequency of physical cash transactions can facilitate the movement and concealment of illicit funds.

These banks generally have significant global presence and engage in activities such as trade finance, cash management services and correspondent banking. Therefore, a significant volume of cross-border transactions with businesses and customers in other jurisdictions are processed by these banks. This could include cross-border transactions with jurisdictions of higher ML risks, where the banks have to put in place additional risk mitigation measures.

The number of STRs filed by these banks in 2011 was the highest among all financial sub-sectors, which indicates significant exposure to ML risks. This, however, is not unexpected given the relative size of this financial sub-sector, the number of transactions processed, and the generally higher level of awareness of the obligation to report suspicious transactions.

Overall, the ML risks for this financial sub-sector are deemed to be significant due to its size, number of higher-risk and PEP accounts, more cash-intensive nature of its activities and high volume of cross-border transactions.

TF Risks

Full banks and QFBs process a significant volume of cross-border transactions. There is a risk that some of these transactions could have been undertaken for the purpose of financing terrorism. In addition, due to the extensive retail reach of these banks and the larger proportion of higher-risk customers, the risks of TF associated with individuals making small-value and dispersed transactions are inherently higher than in other financial sub-sectors. Their trade finance and correspondent banking businesses can also pose TF and proliferation financing risks.

Overall, TF risks for this financial sub-sector are deemed to be higher due to the cross-border nature of its activities, extensive retail reach, which implies a relatively larger number of higher-risk customers, and its trade finance and correspondent banking activities.

[34] Please refer to the MAS website for more information on the different banking licences: http://www.mas.gov.sg/Singapore-Financial-Centre/Types-of-Institutions/Commercial-Banks.aspx.

AML/CFT Controls[35]

MAS Notice 626[36] on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of banks to take measures to mitigate the risk of the Singapore financial system being used for ML/TF. Guidelines are issued to banks to elaborate on some of the requirements under the Notice. Regulations are also imposed on all FIs in relation to transactions with certain jurisdictions and prescribed persons.

MAS dedicates significant resources to the supervision of ML/TF risks and conducts regular AML/CFT inspections as part of its overall supervision efforts. Based on these inspections, MAS notes that most banks have in place appropriate AML/CFT controls that are commensurate with the nature, scale, and complexity of their business activities. For instance, banks screen their customers, Society for Worldwide Interbank Financial Telecommunication (SWIFT) payments and trade finance transactions against sanctions lists. PEPs and other higher-risk customers are subjected to enhanced customer due diligence (CDD) measures.

Nonetheless, MAS has identified a number of areas for improvement. For example, risk assessments of some customers at the stage of onboarding were found to be inaccurate and some banks did not complete their CDD reviews in a timely manner. More recently, weaknesses have been observed in AML/CFT controls of trade finance and correspondent banking businesses such as inadequate policies and procedures, and insufficient transaction monitoring. All findings are shared with the banks, as well as with their head offices and home supervisors (in the case of foreign banks). In all cases, the banks have to demonstrate that deficiencies identified are effectively rectified in a timely manner. To date, the banks have been prompt in rectifying the deficiencies, investing additional resources, and improving their AML/CFT standards over the years.

Next Steps

MAS has scheduled a number of AML/CFT inspections throughout 2014. Following these inspections, the findings, including common weaknesses and best practices, will be shared with the industry to provide additional guidance to enhance its AML/CFT risk management and control standards.

[35] MAS adopts a consistent approach towards supervising wholesale banks, offshore banks, merchant banks and finance companies as we do for full banks and QFBs. While they come under separate MAS AML/CFT Notices due to their different licence types, the AML/CFT requirements contained in the various AML/CFT Notices are the same. As such, this section is referred to in the following sections for wholesale / offshore / merchant banks and finance companies.

[36] MAS Notice 626 applies to full banks, QFBs, wholesale banks and offshore banks. MAS Notice 1014 applies to merchant banks while MAS Notice 824 applies to finance companies.

BOX ITEM 4A: MAS' RISK-BASED APPROACH TO SUPERVISION

MAS adopts a risk-based approach in its supervision of FIs. This approach is articulated in the public monograph on MAS' Framework for Impact and Risk Assessment of Financial Institutions. At the heart of this framework is the impact and risk model which is used to assess FIs on two aspects annually:

- Impact (relative systemic importance): The impact assessment considers the potential impact that an FI may have on Singapore's financial system, broader economy and reputation, in the event of distress. Related institutions are grouped together for an assessment of their aggregate impact. Generally, the larger the FI's intermediary role in critical financial markets or the economy, or the greater its reach to retail customers, the higher its assessed impact.

- Risk (relative risk profile): The risk assessment examines the inherent risks of the FI's business activities, including ML/TF and proliferation financing risks, its ability to manage and control these risks, the effectiveness of its oversight and governance structure, and the adequacy of its financial resources to absorb losses and remain solvent. The assessment also takes into consideration intra-group linkages, where applicable, between the FI and its related entities, and risks posed by other entities in the group (e.g. for a locally-incorporated banking group, risks posed by significant subsidiaries will be aggregated with the main banking entity and monitored on a consolidated basis). To ensure robustness and consistency, the risk assessments of individual FIs are subjected to a process of peer comparison, challenge and review by other experienced supervisors, or panels of senior and specialist staff for key FIs.

Based on the combined assessments of impact and risk (with the impact component accorded greater weightage), the FI is assigned to one of four categories of supervisory significance, with Bucket 1 FIs supervised most intensely. FIs in Buckets 1 and 2 are supervised more closely with more resources allocated by MAS, subjected to more frequent inspections, and have their risk assessments approved by a more senior level of management.

MAS' risk-based approach encompasses both on-site and off-site supervision. MAS' off-site supervision involves ongoing monitoring of an FI's financial soundness and risk indicators, and developments in its businesses and home country, as well as trends in the financial sector. MAS also reviews the FI's regulatory returns and audit reports, and conducts regular meetings with the FI's management, auditors and home supervisors. Concerns impacting the FI's safety and soundness are followed up expeditiously.

BOX ITEM 4B: MAS' AML/CFT REGULATORY REGIME

Singapore operates a strict and rigorous AML/CFT regime centred on a comprehensive and sound legal, institutional, policy, and supervisory framework. The respective MAS AML/CFT Notices and Guidelines are regularly reviewed and updated to align with the evolving standards set by FATF and other relevant global bodies such as the Basel Committee on Banking Supervision.

ML/TF risks are a significant component of the legal, reputational and regulatory risk of an FI. The FI's management of these risks, along with the effectiveness of risk mitigating controls put in place, are assessed by MAS on an ongoing basis. MAS seeks to identify potential risks at these FIs at an early stage and have these risks pre-emptively addressed before they become serious and require more forceful supervisory intervention. MAS' supervisory efforts includes carrying out on-site inspections; checking on the effectiveness of an FI's governance and internal controls; tracking its business development; reviewing its regulatory returns, audit, risk management and compliance reports; and engaging key stakeholders regularly, such as the board of directors and senior management, risk management and compliance staff, as well as internal and external auditors. MAS also requires all FIs to put in place the necessary CFT controls and processes, including screening against relevant terrorists and sanctions lists (e.g. Regulations issued by MAS to give effect to UNSCRs) and making sure that these lists are updated regularly and on a timely basis.

MAS has the authority to impose a broad range of measures in response to an FI's weak AML/CFT controls and regulatory breaches, including financial penalties, administrative sanctions (warning and reprimand letters) and supervisory measures such as restrictions on operations and revocations of licences. The maximum penalty for failure to comply upon conviction is a fine of up to $1 million per offence. A further fine of $100,000 is levied for every day that the regulatory offence continues after conviction. Several FIs had also been directed to appoint external consultants to conduct a thorough review of their AML/CFT frameworks or asked to increase resources dedicated to this function.

Wholesale Banks, Offshore Banks, Merchant Banks

Introduction

Wholesale banks and offshore banks, like full banks and QFBs, are licensed under and governed by the Banking Act. Wholesale banks operate within the Guidelines for Operation of Wholesale Banks issued by MAS and may engage in a similar range of banking businesses as full banks. However, they cannot accept Singapore dollar deposits of less than $250,000[37]. Offshore banks operate within the Guidelines for Operation of Offshore Banks issued by MAS and engage in the same activities as full and wholesale banks to the extent that their activities are transacted through their Asian Currency Units (ACUs)[38]. Offshore banks also do not carry out Singapore dollar retail banking activities.

Merchant banks are approved under the MAS Act and their operations are governed by the Merchant Bank Directives. Their ACU operations are also subjected to the Banking Act. The typical activities of merchant banks include corporate finance, underwriting of share and bond issues, mergers and acquisitions advisory services, portfolio investment management, management consultancy and other fee-based activities.

At the end of 2012, there were 53 wholesale banks, 37 offshore banks and 42 merchant banks operating in Singapore with combined assets of $710 billion.

ML Risks

Wholesale banks, offshore banks and merchant banks typically deal with high net worth individuals, corporates and other FIs, and thus have a more limited customer reach compared to the full banks and QFBs. Hence, they have a relatively smaller number of higher-risk and PEP customers, and a lower number of STRs filed compared to the full banks and QFBs.

These banks are active in private banking, corporate lending and trade financing activities, which involve significantly fewer physical cash transactions relative to full banks and QFBs. Nonetheless, private banking and trade financing activities generally pose higher ML risks.

Several of these banks have global presence. Correspondingly, the banks process a significant number of cross-border transactions, including those involving jurisdictions of greater ML concern.

TF Risks

Notwithstanding the high volume of cross-border transactions, TF risks arising from this financial sub-sector are mitigated by its limited retail reach. As these banks deal mainly with high net worth individuals, corporates and other FIs, the risks of TF associated with using small-value and dispersed transactions are lower relative to other financial sub-sectors. The number of customers that these banks have deemed to pose higher TF and proliferation financing risks is proportionately lower than that for full banks and QFBs, and the number of STRs filed is also lower.

AML/CFT Controls and Next Steps

The AML/CFT requirements and controls in place and the next steps are similar to those for full banks and QFBs[39].

[37] This is the threshold below which "retail banking" is typically described.

[38] An ACU is a sub-division of a bank's accounts that may be used to book foreign currency transactions. Singapore dollar transactions must be booked in the Domestic Banking Unit.

[39] Please refer to the corresponding portion under the preceding section for Full Banks and Qualifying Full Banks.

BOX ITEM 4C: PRIVATE BANKING IN SINGAPORE

There are around 40 FIs in Singapore (i.e., full banks, wholesale banks, offshore banks and merchant banks) that provide private banking services to high net worth individuals.

The large size of assets, high volume of cross-border transactions, and presence of higher risk and PEP customers in private banking give rise to ML risks. However, these risks are relatively lower than those present for full banks and QFBs, given that private banks have fewer customers, less physical cash transactions and more intensive CDD at the stage of onboarding.

TF risks also exist given the larger number of cross-border transactions, but such risks are also relatively lower than those for full banks and QFBs, as private banking customers are subjected to enhanced CDD, as well as regular and close monitoring of their accounts. Further, private banking activities are typically not low-value transactions.

Private banking activities are subjected to the same AML/CFT regulatory requirements as other banking activities. For example, since Singapore criminalised the laundering of proceeds of serious tax offences from 1 July 2013 (please refer to Box Item 4D below), all banks, including private banks, are now required to conduct a critical tax-risk review of their accounts to assess the tax legitimacy of the assets booked.

MAS has worked with the private banking industry through the Private Banking Industry Group (PBIG) to promulgate the Private Banking Code of Conduct ("the PB Code") and industry sound practices (ISP). MAS has also issued circulars on controls for the private banking industry.

Private Banking Code of Conduct

Developed by the Private Banking Advisory Group (the predecessor to PBIG), the PB Code complements MAS' regulatory efforts, and aims to promote good industry practices, enhance transparency to clients and foster the long-term sustainable growth of the private banking industry in Singapore. It focuses on two key areas, namely competency and market conduct.

- On competency, private banking professionals are expected to pass a common competency assessment called the Client Advisor Competency Standards (CACS) before they can provide any financial advice. The CACS focuses on broadening and deepening the knowledge on financial products and regulations that are relevant to the client advisors.

- On market conduct, the PB Code sets out principles relating to the business conduct of private banks and their staff, covering areas such as ethics, and client and risk management.

Industry Sound Practices

As part of continued efforts to ensure sustainable growth of the private banking industry, PBIG developed ISP to safeguard private banks in Singapore from being used as a harbour for proceeds of tax crimes or as a conduit to disguise the origins and flow of such funds. This development came on the back of new FATF Recommendation to designate serious tax offences as ML predicate offences.

MAS will continue to support the PBIG in its review of the PB Code and ISP from time to time to factor in global and industry developments, and operational experience, to ensure continued relevance to the industry and its practitioners.

BOX ITEM 4D: SINGAPORE'S EFFORTS TO COMBAT TAX-ILLICIT PROCEEDS

Singapore has taken a series of measures to mitigate the risk of our financial system being used as a harbour for tax-illicit funds.

- In October 2011, Singapore announced its intention to designate serious tax offences as ML predicate offences. This was before FATF published its revised Recommendations in February 2012.

- In September 2012, MAS directed FIs to prepare for the designation of serious tax offences as ML predicate offences by undertaking a critical tax-risk review of their existing customer and asset pools.

- On 14 May 2013, Singapore completed its review of the existing EOI framework and announced several significant changes to enhance the regime for the exchange of information for tax purposes ("EOI regime")[40].

- On 1 July 2013, the laundering of the proceeds of serious tax offences was criminalised[41].

Designation of Tax Crimes as ML Predicate Offences in Singapore

The range of tax crimes designated as ML predicate offences is comparable with those of OECD jurisdictions and other key financial hubs such as Australia, Hong Kong, the Netherlands and the United Kingdom.

With the designation, FIs and DNFBPs have incorporated and applied the relevant AML/CFT controls and procedures (including filing of STRs and conducting enhanced CDD measures) to detect and deter tax-illicit proceeds. The relevant authorities are now better able to cooperate on and pursue ML investigations involving tax crimes.

STRs involving tax crimes (tax evasion or tax fraud) which are filed with CAD's STRO are analysed and where appropriate, referred to the Inland Revenue Authority of Singapore (IRAS) for investigations into the tax crimes. CAD will also coordinate with IRAS and investigate any ML offence that may be revealed in the course of investigation.

Where applicable, STRO forwards tax crimes related STRs to its FIU MOU counterparts, and allows its counterparts to on-share the relevant information with their tax authorities. With the designation of serious tax offences as ML predicate offences in Singapore, Singapore is also able to provide MLA to foreign jurisdictions to pursue wilful or fraudulent tax evaders and their criminal proceeds in accordance with our MACMA.

[40] These enhancements comprise: (i) signing the Convention on Mutual Administrative Assistance in Tax Matters; (ii) extending the international EOI Standard to all of Singapore's existing tax agreement partners, without having to update individually our tax agreements with them; (iii) streamlining the process for IRAS to obtain bank and trust information from financial institutions without having to seek a court order; and (iv) concluding a Model 1 Intergovernmental Agreement with the US for the Foreign Account Tax Compliance Act.

Singapore already signed the Convention on 29 May 2013, and has made the necessary legislative amendments to implement the enhancements in items (ii) and (iii) above.

[41] Direct and indirect tax offences under Sections 96 and 96A of the Income Tax Act and Sections 62 and 63 of the Goods and Services Tax Act respectively were included in the Second Schedule of the CDSA with effect from 1 July 2013.

Preventive Measures to Detect and Deter Tax-Illicit Proceeds

To aid FIs in the formulation and implementation of effective controls to detect and deter tax-illicit proceeds, PBIG provided guidance on the essential elements that they should incorporate in their AML/CFT policies and procedures in order to: (i) identify and assess tax risks arising from the conduct of their business; and (ii) manage and mitigate such risks. MAS has directed FIs to undertake a critical tax-risk review of their existing accounts to assess the tax legitimacy of their customer and assets pools, and to take special note of the following:

- FIs are expected not to accept a prospective customer if there are reasonable grounds to suspect that the customer's assets are proceeds of serious crimes, such as illicit monies arising from tax evasion and tax fraud; and

- Where there are grounds for suspicion in respect of an existing customer relationship, FIs are expected to conduct enhanced monitoring and where appropriate, to discontinue the relationship. If an FI is inclined to retain the customer, approval must be obtained from its senior management (with the substantiating reasons for retention properly documented), and the account has to be subjected to close monitoring and commensurate risk mitigation measures.

Arising from the critical tax risk-review, FIs have filed STRs where there was suspicion that the customers' assets were tax-illicit proceeds and a number of accounts have been closed (either due to the FI's initiation or the customer's request).

CAD has also reached out to the financial sector to share red-flag indicators FIs should take note of when assessing the tax-risk profiles of their customers and when conducting their CDD checks, and to provide guidance on the filing of tax crimes related STRs.

Various industry groups have come up with guidelines for their members. For example, the private banking industry in Singapore introduced a set of sound practices on the development and implementation of controls to detect and deter the proceeds of tax crimes. The Singapore Trustees Association (STA) has also issued similar guidelines for trust companies.

Finance Companies

Introduction

Finance companies are licensed under and governed by the Finance Companies Act. Their main business is providing fixed and savings deposit services, as well as credit facilities to individuals and corporates. They are not allowed to offer deposit accounts that are repayable on demand by cheque, draft or order. Finance companies are also not allowed to deal in foreign currencies, gold or other precious metals, or to acquire foreign currency denominated stocks, shares or debt securities. At the end of 2012, there were three finance companies operating in Singapore with combined assets of $15 billion.

ML Risks

Customers of finance companies are more likely to perform cash transactions than those of banks, which could increase its ML risks. However, due to licensing restrictions on dealing in foreign currencies, the business of finance companies is largely domestic. Thus, the ML risks arising from cross-border transactions are lower. The proportion of higher-risk customers that finance companies deal with is also lower than that for banks.

TF Risks

As finance companies deal mainly with individuals and small businesses, the risks of TF associated with small-value and dispersed transactions exist. However, since terrorism risks in Singapore are low and finance companies generally do not undertake cross-border business, the TF risks are also lower. In addition, the number of customers deemed by finance companies to pose higher TF risks is of a significantly lower proportion relative to banks.

AML/CFT Controls and Next Steps

MAS Notice 824 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of a finance company to take measures to mitigate the risk of the financial system in Singapore being abused for ML/TF.

The AML/CFT requirements and controls in place and the next steps are similar to those for the full banks and QFBs[42].

[42] Please refer to the corresponding portion under the section for Full Banks and Qualifying Full Banks.

Money-Changers

Introduction

Money-changing business is the business of buying or selling foreign currency notes and is licensed under the Money-changing and Remittance Businesses (MCRB) Act. As at the end of 2012, there were 382 money-changing licensees operating out of 433 locations[43]. Total business volume for 2012 amounted to $36.8 billion.

ML Risks

ML risks for this sector are inherently high as money-changers handle large amounts of physical cash and transact mainly with walk-in and one-off customers. The large number of customers, including foreigners, and the short time taken to complete individual transactions pose significant challenges in identifying suspicious transactions. This is especially so when transactions can be broken down into multiple transactions of smaller amounts to avoid the thresholds for conducting CDD checks by the licensees.

Nonetheless, money-changing licensees have lower numbers of customers from higher-risk groups, such as those from FATF's identified jurisdictions with unsatisfactory AML/CFT regimes. The proportion of PEPs and PEP-related customers is also negligible. CAD has continually conducted outreach to money-changers and remittance agents to highlight risk areas and provide updates on the relevant laws and regulations. As a result, money-changers and remittance agents continue to be vigilant in monitoring transactions and filing STRs.

TF Risks

Money-changers have extensive retail reach and conduct a substantial number of transactions with overseas customers. This inherent nature of the money-changing industry makes it vulnerable to TF risks. As noted from typologies internationally, it might also be possible for foreign terrorist groups to channel the funds for their activities through Singapore by using money-couriers and "trusted" money-changers.

AML/CFT Controls

MAS Notice 3001 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of money-changing and remittance licensees to take measures to mitigate the risk of the industry being abused for ML/TF. Guidelines are also issued to money-changing and remittance licensees to elaborate on some of the requirements under the MAS Notice 3001.

Supervisory actions have been taken against licensees for regulatory breaches. These include the imposition of fines and the non-renewal or revocation of licences. From 2010 to 2012, MAS imposed composition fines on 14 money-changing licensees and two remittance licensees. The licences of six money-changing licensees and seven remittance licensees were revoked or not renewed due to several breaches of the MCRB Act or MAS Notices and licensing conditions, including the failure to comply with AML/CFT requirements.

All applications for money-changing and remittance licences are assessed based on the character and financial condition of the applicant and whether public interest would be served. MAS also assesses the fitness and propriety of the directors and shareholders

[43] Some licensees operate multiple branches.

of the applicant. In addition, MAS' prior approval is required for persons wishing to become substantial shareholders of a licensee, and for appointments of new partners and directors. All money-changing and remittance licences are subjected to annual renewal.

Given the inherent ML/TF risks in the money-changing and remittance businesses and the increasing sophistication of ML/TF techniques, licensees are expected to implement strong AML/CFT controls commensurate with the nature, size, and complexity of their business activities.

MAS will also convey areas of weaknesses noted during on-site inspections to licensees for rectification. General areas where controls could be strengthened include those relating to the performance of CDD measures, record keeping for audit trail purposes and ongoing monitoring of customers' transactions for unusual and/or suspicious transactions.

Next Steps

MAS' enforcement efforts and supervisory actions will be recalibrated to deter non-adherence to regulatory requirements. More inspections, including AML/CFT thematic inspections, will also be conducted. In addition, there will be continued proactive outreach to licensees, including joint initiatives between MAS and CAD to highlight risk areas and relevant laws and regulations.

Remittance Agents

Introduction

Remittance business is the business of accepting funds for the purpose of transmitting them to persons resident in another country or territory outside Singapore, and is licensed under the MCRB Act. At the end of 2012, there were 77 remittance licensees operating out of 186 locations[44]. Remittance licensees are required to be incorporated as companies with a minimum capital of $100,000. In addition, licensees are required to maintain a security deposit of $100,000 with MAS in respect of each place of business. Total outward remittance and inward remittance volumes for 2012 were $24.1 billion and $995 million respectively.

ML Risks

Remittance licensees typically cater to customers such as individuals, foreign workers, expatriate professionals and small and medium enterprises. The channels used for the remittance of funds to beneficiaries overseas include local and foreign banks, other licensed remittance agents in Singapore, and informal networks such as overseas agents. Beneficiaries generally receive their funds via door-to-door cash delivery, direct credits to their bank accounts or self-collection of the funds at designated outlets. Customers usually settle their transactions in cash. They may also use cash cheques or make deposits directly into the licensees' bank accounts.

The cash intensive nature of remittance transactions and the industry's ability to process a large number of transactions cheaply and speedily attract potential money launderers to use remittance agents to move illicit funds. Cross-border fund flows also bring about a greater risk of illicit funds being introduced into the financial system. For instance, there have been cases where proceeds derived from cheating offences and online fraud were transferred to Singapore through remittance agents.

[44] Some licensees operate multiple branches.

The informal overseas networks that some remittance agents use to remit funds may not be adequately regulated in the overseas jurisdictions for AML/CFT purposes. In addition, overseas remittance agents that transact with our remittance licensees often do not disclose the identity of their overseas customers or sources of funds. Consequently, this may increase the industry's exposure to ML risks. In particular, smaller remittance agents may not have adequate resources and systems to put in place additional risk mitigation measures. Common control weaknesses noted in remittance agents include failure to conduct comprehensive CDD and to establish the source of funds, as well as inadequate processes for identifying unusual and/or suspicious transactions. However, as in the case for money-changing licensees, it is noted that remittance licensees do not have a large proportion of customers from higher-risk groups such as PEPs and those from FATF's identified jurisdictions with unsatisfactory AML/CFT regimes.

Overall, the ML risks for remittance agents are relatively higher than other financial sub-sectors in light of the common use of cash, higher exposure to overseas customers, use of informal overseas networks which may not be regulated and the international typologies noted.

TF Risks

Remittance businesses deal mainly with individuals and small businesses and process significant number of international transactions, particularly to jurisdictions within the region. The retail reach, ease and speed of delivery of the funds particularly to the unbanked segment through cash delivery or cash pick-up increases the complexity of tracing the flow of funds. In addition, the use of small-value and dispersed transactions, which is an inherent feature of the remittance industry, may increase the risk that some funds could be inadvertently used for TF.

Transactions with customers who pose higher risks, such as those from FATF's identified jurisdictions with unsatisfactory AML/CFT regimes, are low.

AML/CFT Controls and Next Steps

The existing AML/CFT controls and next steps are similar to those for money-changers[45].

[45] Please refer to the corresponding portion under the preceding section for Money-Changers.

Direct Life and Composite Insurers

Introduction

Singapore's life insurance market is well-developed with a combination of international and homegrown insurers serving the local and expatriate population. Direct life insurers are licensed to write life policies, as well as long- and short-term accident and health policies. Composite insurers write both direct life and general business. At the end of 2012, there were 19 direct life and composite insurers ("DL insurers") operating in Singapore with assets totalling $137 billion which constitute over 80% of the assets of all insurers located in Singapore[46]. DL insurers sell a number of products such as whole life insurance, term insurance, annuities, endowment insurance and investment-linked products. The ML risks for each type of insurance product differ, depending on the nature of the product.

ML Risks

Although this financial sub-sector is much smaller than the banking sub-sector in terms of value and volume of transactions, ML risks may be presented by certain products such as life insurance products with single premium payments and high cash values upon surrender. Products with no cash value, such as term policies, pose lower risks. Money could also be laundered through the assignment of policies and payments to third parties.

DL insurers have a wide retail reach and generally sell most of their policies to individuals. Premium payments are generally made via electronic transfers or cheques. Cash payments may be accepted but are limited to certain amounts. As DL insurers write largely Singapore on-shore risks[47], the risk of foreign illicit funds flowing directly into the life insurance industry is lower. The majority of policyholders are local residents, followed by expatriate professionals working in Singapore.

DL insurers are required to identify customers who pose higher ML risk to their business, including PEPs. The proportion of PEPs and higher-risk customers relative to the customer base as identified by the DL insurers is relatively small. Some of the indicators that DL insurers consider include purchases of large single premium policies, customers who assign policies right after policy inception and customers who surrender large value policies early.

The number of STRs submitted by DL insurers is the highest after the banking sub-sector. However, this does not necessarily mean that ML risks are high, as some DL insurers adopt a conservative approach in reporting suspicious transactions.

TF Risks

The risks of TF for DL insurers are generally lower than the Other Insurers sub-sector (see next section), which has a much greater proportion of off-shore business.

AML/CFT Controls

MAS Notice 314 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the AML/ CFT obligations of a DL insurer. MAS has also issued additional guidance on the requirements under the Notice.

MAS expects DL insurers to observe and scrutinise the conduct of the customer's life policy transactions to ensure that they are consistent with a DL insurer's knowledge of the customer, its business and risk profile, and where appropriate, its source of funds. Currently, DL insurers fulfil such obligations via the use of exception reports and red-flag indicators to identify suspicious transactions.

[46] The insurers located in Singapore are DL insurers, direct general insurers, reinsurers, captive insurers, marine mutuals and Lloyd's service companies.

[47] Off-shore business only accounts for 3% of the total life insurance assets of DL insurers.

Based on MAS' inspections, MAS notes that most DL insurers have put in place AML/CFT controls that are generally commensurate with the nature, size and complexity of their business activities. However, the robustness of their enhanced CDD measures and the rigour with which CDD measures are performed could be strengthened. For example, DL insurers can improve their reviews of customers flagged out by screening systems as potential PEPs or sanctions lists matches, and better determine their customers' sources of wealth. Ongoing reviews of business relationships with existing PEPs and the escalation of such reviews to senior management could also be enhanced. DL insurers have generally been proactive in rectifying the lapses and deficiencies identified by MAS in a timely manner. MAS' inspection reports are shared with the insurers, their head offices or parent companies and their home regulators.

Since January 2013, MAS Notice 123 on Reporting of Suspicious Activities and Incidents of Fraud requires all licensed insurers to report the discovery of any suspicious activities and incidents of fraud to MAS within five working days. This supplements the enhancements made in November 2012 to MAS' Guidelines on Risk Management Practices for Insurance Business – Insurance Fraud Risk. These enhancements provide more explicit expectations regarding the management of insurance fraud risk by insurers with an emphasis on the responsibilities of an insurer's board of directors and senior management, as well as the expectation for insurers to inform MAS about fraud cases they encounter in a timely manner. These ensure that MAS remains constantly updated on the suspicious transactions and incidents of fraud encountered by insurers.

Next Steps

MAS will continue to conduct AML/CFT inspections and share the findings, including common weaknesses and best practices, with the industry to provide additional guidance to enhance their AML/CFT risk management and control standards.

Other Insurers

Introduction

Besides DL insurers, there are also the international and local direct general insurers, reinsurers, captive insurers, marine mutuals and Lloyd's service companies that write both on-shore and off-shore risks ("Other Insurers"). This financial sub-sector is well-developed and diversified.

Insurers from this sub-sector sell a variety of products. Direct general insurers sell retail products such as personal property, travel and motor insurance, and commercial line products such as marine cargo and trade credit insurance. Reinsurers insure other direct general and life insurers' risks while captive insurers insure their own related entities' risks. Marine mutuals insure members' marine business and Lloyd's service companies underwrite specialised third-party risks.

ML Risks

The products sold by this financial sub-sector typically have no cash values and no payouts are made upon maturity of the policies. The nature of these products presents low ML risks.

TF Risks

Compared to other FIs such as banks, Other Insurers have lower TF risks as the insurers pay claims only if the specific insured event occurs. However, TF may still occur when monies obtained through these policies are used to fund illegal activities[48]. Other Insurers also underwrite a relatively large proportion of off-shore risks in terms of gross premiums, although the percentage of higher-risk customers and the number of STRs filed remain very low. In the case of reinsurers, there could also be additional risks if an insurer deliberately places terrorist funds with legitimate reinsurers to disguise the source of funds.

[48] For example, terrorists may make fraudulent claims, request for refund of premiums overpaid or policies cancelled, use workers' compensation payments to support terrorists awaiting assignment, or purchase primary coverage and trade credit insurance for the transport of terrorist materials.
[Source: The International Association of Insurance Supervisors' Application Paper on Combating ML and TF (http://www.iaisweb.org/view/element_href.cfm?src=1/20141.pdf).]

CFT Controls

Similar to DL insurers, MAS develops an understanding of the activities, products and services offered by Other Insurers in Singapore through reviews of external and internal auditors' reports and regular interactions with the insurers. Risk assessments of each insurer are performed regularly. MAS' Guidelines on Risk Management Practices for Insurance Business – Insurance Fraud Risk and MAS Notice 123 on Reporting of Suspicious Activities and Incidents of Fraud also apply to Other Insurers.

Next Steps

MAS will continue to monitor the risks and controls of Other Insurers through off-site supervision, company visits and on-site inspections. MAS will be providing additional guidance to enhance the risk management and control standards of Other Insurers relating to CFT.

Insurance Brokers

Introduction

Direct insurance and reinsurance brokers (IBs) are regulated under the Insurance Act (IA). FIs conducting the following activities as an agent for their customers, in respect of policies relating to general business and long-term accident and health policies (other than policies relating to reinsurance business) or reinsurance of liabilities under policies relating to life business or general business, are required to obtain a registration status, unless otherwise exempted under Section 35ZN of the IA (Exempt IBs):

(i) Receiving proposals for, or issuing, policies in Singapore;
(ii) Collecting or receiving premiums on policies in Singapore; or
(iii) Arranging contracts of insurance in Singapore.

Exempt IBs include licensed financial advisers under the Financial Advisers Act and holders of a Capital Markets Services licence under the Securities and Futures Act (SFA). Please refer to the risk assessments of these sub-sectors in subsequent sections.

At the end of 2012, there were 65 registered IBs. They provide broking services in respect of direct and general insurance policies to their clients, and the sub-sector comprises a mix of small local brokers and mid-to-large sized international insurance broking companies.

ML Risks

IBs act on behalf of their customers to source for insurance coverage from (re)insurers. As general (re) insurance products are needs-based in nature and do not have any cash value unless there is a claim, the risks of ML are much less prevalent in the general insurance and reinsurance broking industry.

TF Risks

Given that IBs have an international client base and source for (re)insurance covers from insurers based in Singapore and overseas, a significant portion of the (re)insurance broking business in Singapore involves cross-border transactions. Notwithstanding this, TF risks are largely mitigated as IBs have very limited exposure to higher-risk customers.

CFT Controls

IBs are required to monitor transactions and report suspicious transactions to STRO promptly. In addition, IBs are aware of their obligations to put in place the necessary CFT controls and processes, and most have duly screened their customers against the UN lists of terrorists, terrorist organisations and other designated entities.

Next Steps

MAS will share good practices and highlight any common weaknesses noted to raise the sub-sector's awareness of IBs' exposure to ML/TF risks and the need for compliance with CFT requirements.

Fund Management Companies

Introduction

Fund Management Companies (FMCs) carrying out the regulated activity of fund management[49] have to be either licensed or registered under the SFA. As at the end of 2012, there were 691 FMCs operating in Singapore, comprising 142 licensed FMCs, 22 registered FMCs and 527 FMCs transitioning from the (now repealed) exempt fund manager framework. With the implementation of the enhanced fund management regime[50] on 7 August 2012, FMCs under the exempt framework must either apply for a licence or register with MAS in order to continue with the regulated activity of fund management.

ML Risks

As an international financial centre, a relatively large proportion of assets under management in Singapore is sourced from investors outside Singapore. Accordingly, the fund management industry frequently engages in a relatively high volume of cross-border transactions. However, these transactions are not carried out by FMCs themselves, but via brokers or banks that are also subjected to AML/CFT obligations and would serve as a second layer of CDD checks. The activities carried out by FMCs also do not involve physical cash.

[49] Fund management is defined under the SFA as undertaking on behalf of a customer (whether on a discretionary authority granted by the customer or otherwise): (i) the management of a portfolio of securities or futures contracts; or (ii) foreign exchange trading or leveraged foreign exchange trading for the purpose of managing the customer's funds. This does not include real estate investment trust management.

[50] As set out in the MAS Annual Report 2012/2013, the enhanced regime aims to raise regulatory standards and supervisory oversight of the fund management industry. Smaller fund managers that were previously exempt as they serve restricted numbers of qualified investors now have to apply for a licence or register with MAS. To qualify for a licence or registration, they have to meet admission criteria such as capital and competency requirements. In addition, enhanced business conduct requirements apply to all fund managers under the enhanced regime. Notwithstanding that the fund management sub-sector is large and diverse with a wide range of fund structures and product offerings to cater to a broad array of investors, the assessment of ML/TF risks has been undertaken for the industry as a whole.

The FMCs licensed by or registered with MAS typically serve accredited or institutional investors, including foreign FIs with their own AML/CFT obligations. Where funds managed by FMCs in Singapore are made available to retail investors, they are typically sold via distributors that are MAS-regulated FIs, such as banks, financial advisory firms and insurance companies, which are required to comply with AML/CFT requirements. Additionally, the fund management industry has a relatively small exposure to higher-risk customers such as PEPs.

TF Risks

Notwithstanding the relatively high volume of international transactions, TF risks arising from this industry are mitigated by its limited direct retail reach, which reduces the risk of TF associated with the use of small-value and dispersed transactions. The proportion of customers in the fund management industry identified as higher-risk such as PEPs is also relatively small.

AML/CFT Controls

The AML/CFT obligations for FMCs are set out in MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism.

FMCs also have to meet minimum eligibility criteria which are tailored to the size and scale of their business activities before they are permitted to carry out fund management activities in Singapore. These criteria relate to the fitness, propriety and competency of an applicant's senior management and shareholders, the financial soundness of the applicant, and the adequacy of its internal controls.

Inspections carried out on licensed fund managers between 2011 and 2013 indicate that FMCs largely comply with MAS Notice SFA04-N02 and Regulations in relation to AML/CFT practices, including enhanced CDD. However, the inspections carried out on exempt FMCs (currently transitioning to become registered or licensed FMCs) indicate a few areas where controls could be strengthened. These areas relate to carrying out enhanced CDD for PEPs, ongoing monitoring of customer accounts, formalising policies and procedures for CDD and record keeping for audit trail purposes.

FMCs are expected to ensure that: (i) they have comprehensive policies and procedures for AML/CFT controls; (ii) the level of CDD performed (at the stage of onboarding and on an ongoing basis) is appropriately suited to a customer's risk profile; (iii) enough efforts are taken to monitor transactions and to report suspicious transactions; and (iv) the board of directors and senior management are appropriately involved in overseeing the AML/CFT controls that the companies have in place.

Next Steps

MAS will also share the key findings from MAS' inspections, including best practices and common weaknesses, with the industry to provide them with guidance on enhancing AML/CFT risk management and control standards.

Trust Companies

Introduction

Trust companies are licensed under the Trust Companies Act (TCA) which came into effect on 1 February 2006[51] and is administered by MAS. Under the TCA, a licence is required for any person carrying on a "trust business". This is defined under the TCA as:

(i) Creating an express trust;
(ii) Acting as trustee for an express trust;
(iii) Arranging for any person to act as trustee for an express trust; or
(iv) Providing trust administration services for an express trust.

Singapore's trust industry has grown steadily along with the growth in the wealth management industry. From 2009 to 2012, the number of Licensed Trust Companies (LTCs) operating in Singapore grew from 40 to 51.

ML Risks

A trust is a common law vehicle that separates the legal ownership of an asset from its beneficial ownership. It is created by a settlor, which is the person who "settles" assets in trust for selected beneficiaries. In creating the trust, the settlor transfers the legal title to the trust assets to a trustee, who then holds and in many cases, manages the trust assets for the benefit of the beneficiaries. The trust structure thus gives rise to opacity as to who actually owns these assets as legal ownership on record lies with the trustee.

While a majority of trust structures are likely set up for legitimate purposes (e.g. succession planning), the potential for abuse exists. It is possible to use trust structures to create layers that obscure the link between illicit monies and their origins. For instance, a perpetrator receiving ill-gotten funds may transfer these funds to a trust structure where the trustee holds and administers the funds for the benefit of the perpetrator's associates. This allows the perpetrator to avoid holding the funds in his own name, while still maintaining some control over the funds through his associates. Furthermore, a trustee may incorporate asset-holding companies to hold trust assets for various administrative reasons. Such corporate structures create additional layers that increase the trust structure's opacity (particularly if the asset-holding company is incorporated in a jurisdiction where information on its shareholders and directors is not readily available), thereby impeding tracing efforts. Perpetrators may also set up complex trust and corporate structures across multiple jurisdictions to make tracing a challenge for enforcement authorities.

A further dimension related to the risks above is the fact that trust services provided by LTCs in Singapore are generally part of wealth management services for high net worth individuals, some of whom could be higher-risk customers such as PEPs.

The Singapore trust industry sees a high volume of cross-border transfers as a relatively large proportion of assets under trusteeship and/or administration in Singapore is from trusts constituted overseas. The transfers of financial assets are, however, not carried out by LTCs themselves but by FIs such as banks. Thus, there is an additional layer of AML/CFT monitoring and gatekeeping by MAS-regulated FIs before the funds of trust customers can enter the Singapore financial system. Additionally, despite the international nature of its activities, LTCs do not carry out physical cash transactions.

[51] Prior to 1 February 2006, trust companies in Singapore were regulated by the Accounting and Corporate Regulatory Authority (ACRA) under the old TCA which was a voluntary registration regime. Under the new regulatory framework, licensing is mandatory. Higher standards of regulation and supervision have also been established to ensure high standards of business conduct, professionalism and competence in the trust industry.

TF Risks

Although LTCs serve accredited and institutional investors rather than retail investors, they could still be vulnerable to TF risks in view of the larger number of higher-risk and PEP trust relevant parties (defined below) associated with LTCs in Singapore, and the prevalence of cross-border transactions in the trust industry.

AML/CFT Controls

Notwithstanding that LTCs fall within the category of DNFPBs under the FATF Recommendations, MAS has imposed regulatory requirements on LTCs which are equivalent in standard to that imposed on other FIs regulated by MAS. LTCs have to meet minimum eligibility criteria relating to the fitness, propriety and competency of their senior management and shareholders, and adequacy of internal controls, as well as other requirements such as financial soundness, before they are permitted to provide trust business services in Singapore.

Specifically, MAS Notice TCA-N03 on Prevention of Money Laundering and Countering the Financing of Terrorism prescribes the AML/CFT obligations of LTCs. MAS Notice TCA-N03 requires LTCs, *inter alia*, to conduct CDD on "trust relevant parties", which includes the settlor, the beneficiaries and the trustee. For example, an LTC has to identify and obtain the particulars of (using reliable independent sources):

(i) The settlor before the trust is constituted; and
(ii) Each beneficiary before making a distribution to that beneficiary.

Where the trust relevant party is a PEP, the LTC must conduct enhanced CDD, including establishing the source of wealth/funds via appropriate and reasonable means. Over and above this, LTCs are also subjected to the obligation to detect and report suspicious transactions.

A breach of these obligations by an LTC is sanctionable and criminal sanctions can also be imposed. An LTC's adherence to these requirements also comes under review during MAS' periodic inspections. The stringent regulatory standards to which LTCs in Singapore are held hinder the ability of perpetrators to use LTCs here to create or administer trust structures that conceal illicit funds.

In addition, MAS works with the industry to maintain the standards. Recently, STA, Singapore's trust industry association, issued industry guidance to LTCs on 19 June 2013 on procedures that could be implemented to enhance compliance with the new FATF Recommendation to designate serious tax offences as ML predicate offences in Singapore.

MAS issued two circulars in 2008 and 2013 to the industry, highlighting both common weakness and best practices that it had observed from its AML/CFT thematic inspections in the past six years. No lapse was noted in relation to enhanced CDD for higher-risk such as PEP trust relevant parties. Areas where controls could be strengthened relate to documentation of policies and procedures and the audit trail relating to CDD.

Next Steps

LTCs are assessed to be more vulnerable to ML/TF risks compared to other non-bank FIs, notwithstanding the controls in place. Accordingly, MAS expects LTCs to maintain the strength of their AML/CFT controls.

The findings, common weaknesses and best practices, identified through MAS' inspections of LTCs, will continue to be shared with the trust industry to provide additional guidance to enhance their AML/CFT risk management and control standards.

Broker-Dealers

Introduction

The licensed broker-dealers sub-sector is regulated under the SFA. FIs conducting any of the following regulated activities are required to hold a capital markets services licence, unless otherwise exempted under Section 99 of the SFA ("Exempt FIs"):

(i) Dealing in securities;
(ii) Trading in futures contracts;
(iii) Leveraged foreign exchange trading;
(iv) Securities financing; or
(v) Providing custodial services for securities.

Exempt FIs include banks licensed under the Banking Act or approved under the MAS Act and finance companies licensed under the Finance Companies Act. Please refer to the respective risk assessments of these sub-sectors.

At the end of 2012, there were 89 licensed broker-dealers conducting one or more of the five regulated activities listed above. The business models of these licensed broker-dealers vary in size and complexity, ranging from small firms acting as introducing brokers[52] to large corporations with exchange clearing memberships[53].

ML Risks

The ML risks generally associated with licensed broker-dealers arise from the layering of illicit funds facilitated by the high transactional speed and ease of global reach. In Singapore, the sub-sector is characterised by a large number of retail accounts and high cross-border transaction volumes, which increase the difficulty of effectively monitoring possible ML activities. However, the ML risks are largely mitigated by the fact that the licensed broker-dealers have limited exposure to higher-risk customers such as PEPs. Moreover, the amount of physical cash receipts relative to the total amount of customers' funds handled by licensed broker-dealers is small.

The number of STRs filed by the sub-sector is relatively higher compared to some other sub-sectors, which could indicate significant exposure to ML risks. However, this is not unexpected given the large number of transactions involved and the higher level of awareness among licensed broker-dealers regarding suspicious transactions reporting.

TF Risks

The high cross-border transaction volumes handled by licensed broker-dealers could expose the sub-sector to TF risks. However, given the limited exposure to higher-risk customers and the stringent controls on third-party payments and receipts, the TF risks are largely mitigated. Nonetheless, an area of concern is the sub-sector's wide retail reach where terrorist financiers could, for example, exploit unknowing individuals and use their trading accounts opened with the licensed broker-dealers to mask illicit cross-border wire transfers.

AML/CFT Controls

MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of the licensed broker-dealers to take the necessary measures to mitigate the risk of the capital markets in Singapore being abused for ML/TF activities. Further guidance is provided in MAS' Guidelines to MAS Notice SFA04-N02. TF-related Regulations, including restrictions on transactions with certain jurisdictions and designated entities, are also issued to all FIs. A breach of the requirements of the Notice and relevant Regulations is sanctionable.

[52] For the purpose of dealing in securities, an introducing broker refers to a corporation which does not carry customers' positions, margins or accounts in its own books, and either: (i) carries on the business only of soliciting or accepting orders for the purchase or sale of securities from any customer (not being a restricted broker); or (ii) accepts money or assets from any customer as settlement of, or a margin for, or to guarantee or secure, any contract for the purchase or sale of securities by that customer.

[53] A clearing member refers to a corporation which is a member of an approved clearing house authorised to operate a clearing facility for securities or futures contracts.

The AML/CFT control measures undertaken by licensed broker-dealers are generally satisfactory. Nevertheless, licensed broker-dealers are expected to enhance their control measures continually given the increasing sophistication of ML/TF techniques. Based on MAS' on-site reviews, most licensed broker-dealers have systems in place to conduct adequate CDD for account opening and set appropriate parameters for ongoing transaction monitoring. Enhanced CDD is also applied to higher-risk customers such as PEPs.

In instances where licensed broker-dealers handle physical cash, or when funds are wired into or out of jurisdictions known to be more susceptible to ML/TF risks or with AML/CFT deficiencies, additional AML/CFT controls have been put in place. For example, licensed broker-dealers would enquire about the source of funds and the reason for large cash payments. An STR would be filed if the customer is not able to provide valid reasons for large physical cash transactions. The customer may also be tagged as posing higher risks and be subjected to enhanced ongoing monitoring.

Next Steps

MAS will continue its supervisory engagement of licensed broker-dealers through both on-site and off-site reviews, industry engagements and sharing of good practices and common weaknesses noted.

Corporate Finance Advisory Firms

Introduction

The corporate finance advisory sub-sector is regulated under the SFA. FIs conducting corporate finance advisory activities are required to hold a capital markets services licence ("CF Firms"), unless otherwise exempted under Section 99 of the SFA.

FIs conducting corporate finance advisory activities but exempted from licensing include banks licensed under the Banking Act or approved under the MAS Act and finance companies licensed under the Finance Companies Act. Please refer to the respective risk assessments of these sub-sectors.

As at the end of 2012, there were 24 CF Firms. They are involved in the provision of advice to any person concerning fund-raising, making an offer to subscribe for or dispose of securities, corporate take-overs and business restructuring.

ML Risks

The number of CF Firms in Singapore is small relative to other sub-sectors. They provide advisory services primarily to institutional and accredited investors. The ML risks arising from dealing with higher-risk customers such as PEPs are not significant.

CF Firms generally do not undertake transactions on behalf of their customers. If they carry out any form of underwriting or placement of securities, they are also required to be licensed to perform the regulated activity of dealing in securities under the SFA[54]. Consequently, they do not typically handle customers' funds in the course of their business, and transactions between the CF Firms and their customers are limited to advisory fee payments, which flow through Singapore's banking and payments infrastructure. CF Firms have also indicated that they do not handle physical cash receipts from customers.

Notwithstanding the above, money launderers could possibly rely on bona fide corporate finance advice to layer illicit funds by participating in corporate finance deals, such as corporate take-over deals which involve substantial funds from investors.

TF Risks

Given the advisory nature of the business and that CF Firms do not handle customers' funds. TF risks are not prevalent in this sub-sector.

AML/CFT Controls

MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of CF Firms to take the necessary measures to mitigate the risk of the capital markets in Singapore being abused for ML/TF activities. Further guidance is provided in MAS' Guidelines to MAS Notice SFA04-N02. TF-related Regulations, including restrictions on transactions with certain jurisdictions and designated persons, are also issued to all FIs. A breach of the requirements of the Notice and relevant Regulations is sanctionable.

The AML/CFT control measures put in place by CF Firms are generally satisfactory. Based on MAS' on-site reviews, most CF Firms have policies and procedures in place to conduct adequate CDD when undertaking a new mandate, such as applying enhanced CDD on higher-risk customers such as PEPs. CF Firms are also required to take the appropriate measures to detect unusual and/or suspicious transactions and file STRs. The sub-sector's ML risks are further mitigated by the fact that investment funds designated for corporate finance transactions are generally subjected to a primary layer of AML/CFT checks by the banks at the point of deposit, payment or transfer.

Next Steps

MAS will continue its supervisory engagement of CF Firms through both on-site and off-site reviews, industry engagements and sharing of good practices and common weaknesses noted.

[54] Please refer to the section on Broker-Dealers.

Financial Advisers

Introduction

The financial advisory sector is regulated under the Financial Advisers Act (FAA). FIs conducting the following regulated activities are required to hold a Financial Advisers' licence, unless otherwise exempted under Section 23 of the FAA ("Exempt FIs"):

(i) Advising others directly or through publications or writings concerning any investment product;
(ii) Advising others by issuing or promulgating research analysis or reports concerning any investment product;
(iii) Marketing any collective investment scheme; or
(iv) Arranging any contract of insurance in respect of life policies.

Exempt FIs include banks licensed under the Banking Act or approved under the MAS Act, finance companies licensed under the Finance Companies Act, insurance companies licensed and insurance brokers registered under the Insurance Act and holders of a capital markets services licence under the SFA. Please refer to the respective risk assessments of these sub-sectors.

As at the end of 2012, there were 62 licensed financial advisers (FAs). FAs are involved in providing investment advice, marketing unit trusts and arranging life insurance policies.

ML Risks

The customer base of FAs comprises mostly retail investors, with the sub-sector having limited exposure to higher-risk customers such as PEPs. The large number of accounts increases the difficulty of effectively monitoring possible ML activities. However, this is mitigated by the fact that FAs are primarily in the business of providing advice and are typically not allowed to handle customers' funds or undertake investment transactions on behalf of their customers. Where FAs do receive customers' funds, either from local or overseas customers, the funds are mainly for life insurance policies. The funds primarily flow through Singapore's banking and payments infrastructure, which is likewise subject to MAS' AML/CFT requirements.

TF Risks

Given the advisory nature of the business and that FAs generally do not handle customers' funds. TF risks are not prevalent in this sub-sector. FAs also have very limited exposure to higher-risk customers such as PEPs compared to other sub-sectors.

AML/CFT Controls

MAS Notice FAA-N06 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations of FAs to take the necessary measures to mitigate the risk of the financial advisory industry in Singapore being abused for ML/TF activities. Further guidance is provided in MAS Guidelines to MAS Notice FAA-N06. TF-related Regulations, including restriction on transactions with certain jurisdictions and designated entities, are also issued to all FIs. A breach of the requirements of the Notice and relevant Regulations is sanctionable.

Notwithstanding the lower ML/TF risks of this sub-sector, MAS' on-site reviews have shown that the AML/CFT controls of some FAs have room for improvement. Weaknesses noted include lack of policies and procedures for updating of customer information and for conducting enhanced CDD for PEPs, as well as inadequate monitoring and review of dormant accounts and suspicious transactions. MAS has taken the necessary and appropriate supervisory measures. Given the inherent risks arising from the sub-sector's business operations and the increasing sophistication of ML/TF techniques, FAs need to place more emphasis on strengthening their AML/CFT controls.

Next Steps

MAS will continue its supervisory engagement of FAs through both on-site and off-site reviews, industry engagements and sharing of good practices and common weaknesses noted.

Stored Value Facility Holders

Introduction

Stored value facilities (SVFs), as set out in the Payment Systems (Oversight) Act 2006 (PS(O)A), are prepaid payment products that can be used for making payments for goods and services up to the amount of the stored value that has been prepaid. Such payments are made by the SVF holder rather than by the user. SVFs can be provided in different forms such as smart cards, contactless cards, paper vouchers, and internet-based SVF accounts.

ML/TF Risks

Internet-based SVFs[55] are typically used for purchasing goods and services from online merchants acquired by the SVF holder. Such SVFs may also be used to facilitate person-to-person payments.

ML/TF risks arise from the international nature of internet-based transactions as cross-border acceptance of payments can be attractive to money launderers. Cross-border enforcement of ML/TF offences can be challenging, especially in cases where the internet-based SVF holders offer services to persons outside the jurisdiction where it provides the services.

The anonymity accorded by internet-based SVFs, both at the user identification and transactional level, also makes them vulnerable to ML/TF. Given the nature of the internet business, face-to-face contact may be

[55] For the purposes of this section, the term "internet-based SVFs" refers to prepaid internet-based payment services which are considered SVFs under the PS(O)A.

limited or absent. This may increase identity-related risks such as impersonation fraud. SVF holders who require the submission of customer data may also face challenges in identity verification. In addition, though not a risk exclusive to the internet-based SVF sub-sector, inadequate record keeping of customer data and transaction records may lead to increased ML/TF risks.

Another source of ML/TF risks is anonymous funding of internet-based SVFs. Anonymous funding methods may include loading funds directly through cash deposits, money orders or fund transfers from other anonymous SVFs. Anonymous funds may also be provided by third parties other than the registered users of internet-based SVFs, depending on the controls imposed by the holders. ML/TF risks would also be higher if stored value and transaction limits are not imposed by internet-based SVF holders.

AML/CFT Controls

MAS Notice PSOA-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism is applicable to holders of SVFs that are able to contain a stored value of not less than $1,000. The Notice sets out the obligations of SVF holders to conduct CDD, maintain records and report suspicious transactions, among other AML/CFT requirements.

In addition to the MAS Notice PSOA-N02, MAS has issued a set of SVF Guidelines which contain broad principles on the sound practices and risk mitigation measures that holders should adopt in relation to their SVFs. These Guidelines apply to all SVFs and address important issues such as transparency, disclosure, public confidence, stored value protection and AML/CFT requirements. The Guidelines also set out recommendations in respect of bulk purchases, the transfer of stored value from other anonymous SVFs, and maintenance of audit trails. SVF holders are also expected to maintain proper records of all SVF sales and transactions. SVF holders are strongly encouraged to adopt and implement these Guidelines, while taking into consideration the nature, size and complexity of their SVFs.

Next Steps

MAS monitors the issuance of open-loop prepaid cards in Singapore, such as those based on well established and widespread technical standards (e.g. Visa, MasterCard and American Express). At present, there are limited ML/TF risks arising from such Singapore-issued cards, which have limited circulation, functionalities, and self-imposed limits of low value. Such cards would be subjected to MAS Notice PSOA-N02 if their stored value limits are raised.

Under the existing regulatory framework, holders of SVFs are not subject to inspections. Nonetheless, MAS continues to monitor new and emerging SVFs and will identify ML/TF risks that may be of concern. If necessary, MAS will consider additional steps to deal with such issues.

Risks to Study Further

Virtual Currencies

Virtual currencies, such as bitcoins and precious metal-backed digital currencies are examples of emerging internet-based non-physical representations of value that can be exchanged for goods and services at places that accept them. These virtual currencies are usually not denominated in fiat currency and can typically be transferred electronically from one user to another. Transfers may be facilitated by virtual currency exchanges, which also serve to facilitate the exchange of fiat currency for the various virtual currencies.

Virtual currencies are gaining popularity among online users worldwide. These virtual currencies inherit some of the risks from internet-based payment services due to their anonymity, cross-border nature and low transaction costs. Virtual currencies and virtual currency exchanges may be utilised for illegal activities, including ML/TF.

MAS is closely monitoring developments in this area and will consider the need for regulation if necessary.

5. Non-Financial Sectors Risk Assessment

Casinos

Introduction

Singapore's IRs – Marina Bay Sands and Resorts World Sentosa – were opened in 2010. There are casinos within the two IRs and they are regulated by CRA. The casinos must comply with regulatory requirements as stipulated in the Casino Control Act and its Regulations.

ML Risks

Casino operations are largely cash-based. This presents opportunities for ML, which can occur through large cash buy-ins and pay-outs with minimal gambling or the "exchange of chips" through fictitious gambling activities. Casinos may therefore become conduits for ML when proceeds of crime transferred to casinos are accepted for purposes of gambling and subsequently withdrawn as casino winnings. Casino marketing arrangements made by international market agents (IMAs)[56] may also be vulnerable to ML risks given their intermediary role and the receipt of funds from overseas.

While there are potential ML risks posed by cash activities in the casinos, the act of gambling itself requires funds to be put "at risk". When put "at risk", there is a chance that a significant proportion of their proceeds of crime may be lost as gambling outcomes are random and not predictable. This may help to deter criminals from laundering their proceeds through the casinos. Gambling integrity is an area closely regulated by CRA. Close supervision of gambling integrity is complemented by stringent regulatory requirements imposed on the casino operators to prevent, deter and detect ML activities.

TF Risks

The TF risks to the casinos are assessed to be lower presently. Monies used for gambling would be put "at risk" i.e., terrorist groups will not get the opportunity to "grow" their funds, and this would be a less effective way to raise funds to finance terrorist activities.

AML/CFT Controls

Regulations/Guidelines/Enforcement Mechanism in Place

To mitigate the risks posed by significant cash activities in the casinos, CRA has prescribed preventive and detective measures for cash activities. These include the following:

(i) Casino operators are required to file a cash transaction report to STRO for any cash transaction that involves an amount of $10,000 or more;

(ii) Casino operators are prohibited from entering into any transaction involving the conversion of money from one form to another when the funds are not used for gambling. In addition, casino operators are to determine the purpose and ownership of each cash transfer upon the receipt of such cash transfers, failing which, casinos are prohibited from retaining the funds; and

(iii) Casino operators and their employees are obliged under Section 39 of the CDSA to report any suspicious transaction if they know or have reasonable grounds to suspect that the funds may be related to or represent criminal proceeds.

Cheques and telegraphic transfer payments made by the casino operators have to be identified as either "winnings" or "non-winnings". This helps to prevent individuals from citing casino winnings as their source of funds when depositing funds with FIs.

[56] An IMA is a person licensed by CRA who organises, promotes or facilitates the playing of any game in a casino by one or more patrons, for which the licensed IMA receives a commission or other forms of payment from the casino operator.

Other preventive measures include the requirement to conduct CDD in the following scenarios: -

(i) A patron establishes a patron account with the casino operator;
(ii) A patron enters into a cash transaction involving $10,000 or more in a single transaction with the casino operator;
(iii) A sum of $5,000 or more in a single transaction is deposited into an account;
(iv) The casino operator has a reasonable suspicion that any patron is engaged in ML/TF activities; or
(v) The casino operator has doubts about the veracity or adequacy of any information previously obtained about a patron.

IMAs are licensed by CRA. Patrons of IMAs are required to establish an account with the casino operators and are subject to the same CDD requirements as non-IMA patrons.

Casino operators and IMAs which fail to comply with the regulatory requirements are liable to disciplinary action, which may include suspension or cancellation of the casino or IMA licence.

Professional Ethics/Standards and Integrity of Gambling

To ensure that the integrity of the casinos is not compromised from within, all casino employees performing casino operations are required to obtain a special employee licence under the Casino Control Act. All games offered in the casinos in Singapore have to be approved by CRA and the casino operators have to ensure that the games are conducted in accordance to the game rules approved by CRA to preserve the integrity and randomness of the game. This will minimise collusion between employees and patrons, which in turn will reduce the ML/TF risks arising from collusion.

AML/CFT On-site Inspections and Compliance Monitoring

The casino operators are required to put in place a system of internal controls and procedures that will meet the requirements set out in the Casino Control Act and its Regulations. The casino operators are required to submit their internal controls for approval by CRA.

As part of the process to ensure compliance and for the casino operators to take remedial measures where they are lacking, CRA conducts regular inspections on the casinos' operations. A "full-scope" inspection on both casino operators was conducted by CRA in 2012 on various aspects of the casinos' operations, including their AML/CFT measures. The inspection sought to determine the extent of compliance with the AML/CFT requirements.

Casino operators are also required to check and screen their patrons against the UN lists of terrorists, terrorist organisations and other designated entities. This is required as part of the specific controls imposed to deal with TF risks.

Next Steps

The requirement to conduct CDD will be enacted in the Casino Control Act to emphasise the importance of performing CDD. More prescriptive measures will be included in the Casino Control (Prevention of Money Laundering) Regulations to emphasise the importance of, and demonstrate our commitment to, preventing ML/TF in the casinos. To ensure compliance and effectiveness of these measures, CRA will, from time to time, monitor and inspect the casino operators' implementation of AML/CFT measures to ensure that the casinos have effectively put in place robust AML/CFT controls.

Pawnbrokers

Introduction

The pawnbroking industry caters to individuals who need short-term financial relief and possess valuables that can be pledged, e.g. jewellery and luxury watches. The assets pledged can be redeemed anytime within the redemption period (which must be at least six months). Interest rates are capped by law at 1.5% per month.

The pawnbroking industry has grown substantially since 2008. The number of pawnshops increased from 114 in 2008 to 191 in 2012, with total outstanding loans in excess of $1 billion in 2012[57]. About four million loans were issued in 2012, although this figure includes loans refinanced using the same collateral. Currently, there are three pawnbroking companies with a combined ownership of 71 pawnshops listed on the Singapore Exchange.

ML Risks

Transactions in the industry are mainly cash-based. From both ML and TF perspectives, the industry poses two key concerns: (i) pawners repaying debts using illicit monies; and (ii) pawners pawning fraudulently-obtained pledges and leaving them unredeemed. Gold items are of special concern because they constitute about 90% of all pledges.

These concerns are mitigated by the requirement for pawnbrokers to obtain and keep the particulars of their customers. All loans are disbursed to the pawners, who must be physically present at the pawnshop to pawn their pledges. Pawnbrokers therefore generally know their customers, who tend to be locals. Furthermore, the loan amounts are generally small, with only about 0.20% of loans exceeding $20,000 in 2012.

The instances of illicit pledges being pawned are also relatively rare, with an estimated 600 cases of stolen goods being pawned in 2012, corresponding to less than 0.02% of all loans. These cases mainly relate to isolated instances of opportunistic thefts of low-value items, and are not known to be related to organised criminal or ML/TF activities.

TF Risks

The majority of customers are locals, with foreigners constituting 5% to 30% of all pawners[58]. Hence, the risks of foreign terrorists actually using monies for TF or terrorist activities are moderate to low. Furthermore, a terrorist looking to monetise an asset is more likely to sell it, rather than pawn it.

AML/CFT Controls

There are currently no specific AML/CFT obligations for pawnbrokers. However, pawnbrokers are not allowed to knowingly deal in illicit goods. The particulars of pawners must be recorded and maintained, and screened against UN lists of terrorists, terrorist organisations and other designated entities. Under the Pawnbrokers Act, it is an offence for a person to knowingly pawn someone else's property without authorisation. It is also an offence if a person is unable to satisfactorily account for how he came into possession of the article to be pawned.

[57] Unless otherwise stated, the statistics provided in this section are based on the monthly returns provided by pawnbrokers.

[58] This information is based on a 2012 survey of 50 pawnbrokers.

Pawnbrokers are expected to take proactive and reasonable steps to ensure that the pledges have not been fraudulently obtained, such as requiring a pawner to produce a receipt as proof of purchase, or recording the particulars of a guarantor who shall vouch that the item pawned is not stolen. There is also a mechanism for the police to circulate to pawnbrokers information on property reported as lost, stolen or otherwise fraudulently disposed of, and for the pawnbrokers to look out for such property. If the pawnbroker reasonably suspects that the article has been obtained illegally, he has the power to seize and detain the person offering the article and deliver him with the article into the custody of a police officer. Pawnbrokers are also required to file STRs under the CDSA.

The Insolvency and Public Trustee's Office (IPTO) works closely with the police to ensure that the substantial shareholders and directors are fit and proper to carry on a pawnbroking business. IPTO is also vigilant in keeping the industry free of ethically-questionable people. For example, in 2012, IPTO ordered a majority shareholder of a pawnshop to reduce his shareholding to no more than 20% and as a result, dilute his influence over the pawnbroking business, on account of his conviction under the Secondhand Goods Dealers Act.

Aside from the occasional incident, pawnbrokers have generally conducted themselves well. In 2012, just seven complaints against pawnbrokers were lodged, all involving minor administrative breaches.

Next Steps

IPTO is contemplating the introduction of new AML/CFT requirements into the Pawnbrokers Act in 2014. This will include comprehensive CDD measures to complement the existing record keeping duties pawnbrokers already have. Obligations and guidance relating to the detection of suspicious activities/transactions and filing of STRs are also expected to be expanded to add to the baseline obligations under the CDSA. These new measures will, if implemented, also be subjected to compliance checks conducted by IPTO.

Moneylenders

Introduction

The moneylending industry caters to individuals who need financial relief, but can neither obtain credit from banks nor offer many valuables to pawnbrokers. The vast majority of loans are unsecured, and borrowers with annual income of less than $30,000 are protected by a 20% cap on effective interest rate per annum. There are also limits on the loan amounts:

(i) Four times the borrower's monthly income if his annual income is at least $30,000 but less than $120,000;
(ii) Two times the monthly income if his annual income is at least $20,000 but less than $30,000; and
(iii) $3,000 if his annual income is less than $20,000.

The moneylending industry has grown significantly since 2008, with the number of moneylenders having increased from 173 in 2008 to 209 in 2012[59]. The average annual value of loans given out from 2008 to 2012 is about $350 million. Some 264,000 loans were issued in 2012.

ML Risks

The cash-intensive nature of the industry raises potential ML concerns. However, there are low lending limits and the average loan value is less than $1,500, so the moneylending industry is only moderately attractive as a channel for ML. Nonetheless, unlicensed moneylending is a significant ML threat in Singapore, as noted in Chapter 4 of this report.

TF Risks

Only a relatively small proportion of loans involve foreign borrowers (10% of loans in 2012). Moneylenders are also not known to lend for uses outside of Singapore. Hence, the TF risks of foreign terrorists making use of moneylenders are moderate to low.

[59] The statistics provided in this section are based on the quarterly returns provided by moneylenders.

AML/CFT Controls

The Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009 (PMFTR) came into force in early 2009. The PMFTR requires moneylenders to conduct CDD to identify and verify their customers and beneficial owners, to adopt enhanced CDD for higher-risk customers, and to file STRs etc. Loans to first-time customers are generally disbursed to the borrowers in person. Moneylenders are also required to screen their customers against UN lists of terrorists, terrorist organisations and other designated entities as part of their CFT controls. Moneylenders are also tested on their mastery of the PMFTR and other moneylending laws as a licensing prerequisite.

In 2012, IPTO conducted 81 inspections on moneylenders. Routine audits of each moneylender's loan transactions are also conducted at least once a year. IPTO works closely with the police to ensure that the shareholders, directors, managers and staff of licensees are fit and proper persons who are involved in a moneylending business. In 2012, 10 moneylenders had their licences revoked or not renewed for contravening the moneylending laws, licence conditions or directions.

Next Steps

IPTO will be enhancing its AML/CFT supervisory focus and has stepped up its enforcement of the PMFTR since late 2013. For example, all moneylenders have been directed to submit, by 31 August 2014, an audit report on their internal policies, procedures and controls to detect and prevent ML/TF.

Corporate Service Providers

Introduction

CSPs are business entities and people that provide a range of services such as corporate advisory, office hosting, corporate secretarial services and statutory filings for their customers. The individuals who provide such services are known as "prescribed persons", as defined in the various Acts administered by the Accounting and Corporate Regulatory Authority (ACRA)[60]. Prescribed persons include lawyers, accountants, chartered secretaries and corporate secretarial agents. As of December 2012, there were approximately 2,800 CSP business entities and 3,500 prescribed persons.

One of the core businesses of CSPs is to assist individuals and business entities with the statutory filing of documents with ACRA. These statutory requirements are set out in various ACRA-administered Acts (e.g. applications relating to the incorporation of companies, allotment of shares and filing of annual returns). Since January 2003, documents have to be filed via Bizfile, ACRA's online filing system. While the officers of companies and business owners can perform statutory filings on their own, the majority rely on CSPs to do so.

[60] These Acts are the Business Registration Act, the Companies Act, the Limited Liability Partnerships Act and the Limited Partnerships Act.

ML/TF Risks

Some of the services that CSPs offer to their local and foreign customers would require scrutiny from an AML/CFT perspective. They include CSPs:

(i) Acting as a formation agent of legal persons;
(ii) Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons;
(iii) Providing a registered office, business address or correspondence or administrative address for a legal person or arrangement; and
(iv) Acting as (or arranging for another person to act as) a nominee shareholder for any person other than a corporation whose securities are listed on a securities exchange or a recognised securities exchange under the SFA.

Given that the nature of the services provided by CSPs does not involve large amounts of cash or the actual movement of funds, the risk of CSPs being used directly for ML/TF is relatively moderate. However, CSPs may come across higher-risk customers such as PEPs or persons from or in foreign jurisdictions, including those known to have inadequate AML/CFT measures. The risks could increase if such higher-risk customers engage CSPs to set up complex or unusual structures to conceal beneficial ownership and deliberately reduce the transparency of transactions. There are occasions where a CSP may be engaged by a non-resident person to incorporate a company in Singapore and to provide the services of a locally-based director for that company. While most of such arrangements are for legitimate purposes, the opportunities for abusing the incorporated company for ML/TF activities can arise.

ACRA's overall assessment is that the ML/TF risks in the CSP sector will be significantly reduced with the amendments to the ACRA Act and the introduction of new regulations to enhance the regulatory framework for CSPs.

AML/CFT Controls

There are currently no AML/CFT requirements imposed on CSPs. However, the ACRA Act is being amended to enhance the regulatory framework and require CSPs to have control measures to mitigate the ML/TF risks. ACRA will also be empowered to request for necessary beneficial ownership information from CSPs, to inspect CSPs to ensure their compliance with these obligations and to sanction errant CSPs.

The key control measures to mitigate the ML/TF risks are:

(i) Register only fit and proper persons as CSPs (referred to as filing agents and qualified individuals in the amendments to the ACRA Act);
(ii) Impose obligations on CSPs in line with relevant FATF Recommendations, such as the requirements to conduct CDD, enhanced CDD and transactions monitoring. Registered filing agents will be required to obtain beneficial ownership information and maintain records of such information accordingly, as part of their CDD requirements. This will include business entities and companies set up by foreigners[61] who can only do so with the help of CSPs. Such foreigners will thus be subjected to CDD checks by CSPs, including obtaining of beneficial ownership information.

[61] Foreign persons are unable to register business entities with ACRA directly without engaging the services of CSPs. This is because people are required to have an authentication code known as the Singpass in order to access ACRA's online filing system, Bizfile, and this authentication code is only issued to Singaporeans and permanent residents.

(iii) Introduce enforcement powers for ACRA to inspect a registered filing agent's business premises, obtain documents relating to its filing business, require information to be provided, and audit a registered filing agent's internal policies, procedures and controls;

(iv) Introduce enforcement powers for ACRA to sanction registered filing agents that breach the legal obligations imposed on them, e.g. suspend or cancel their registration, restrict their access or use of Bizfile or impose a financial penalty; and

(v) Require registered filing agents to consider whether to file STRs under the CDSA and the TSOFA if they are unable to apply CDD measures.

In addition, ACRA will disseminate information to CSPs on the requirement to conduct screening of their customers against the UN lists of terrorists, terrorist organisations and other designated entities.

Next Steps

ACRA has formed a working group comprised of representatives from professional bodies that CSPs may belong to. The working group will discuss the internal policies and procedures that CSPs should adopt relating to CDD, ongoing monitoring, record keeping, audit and compliance management, and reporting. The working group will also establish programmes to evaluate compliance with the new legal obligations, provide training and draft guidelines for CSPs.

Real Estate

Introduction

The real estate sector in Singapore has distinct public and private housing segments. Public housing constitutes about 76% of the total housing stock in Singapore and transactions are tightly controlled by the Government through ownership[62] and occupancy restrictions. In comparison, private housing units are mostly freely transacted, along with commercial and industrial properties. However, the volume and value of commercial and industry property transactions are significantly lower than that of private housing[63].

A typical property transaction involves several parties such as the real estate agent, property developer, solicitors and FIs providing the loans to the developers or purchasers.

The estate agent profession is regulated under the Estate Agents Act (EAA), which is administered by the Council for Estate Agencies (CEA). Estate agency businesses are licensed by the CEA and are referred to as estate agents. They include sole-proprietorships, partnerships and companies. Salespersons are individuals who perform estate agency work. Under the EAA, salespersons have to be registered with an estate agent before they can conduct estate agency work. The EAA does not cover direct sales by property developers.

[62] Flats sold by HDB are meant for Singapore citizens who meet the eligibility conditions shown on HDB's website. Please refer to the following link: http://www.hdb.gov.sg/fi10/fi10321p.nsf/w/BuyingNewFlatEligibilitytobuynewHDBflat. Singapore citizens and Singapore permanent residents are allowed to purchase resale HDB flats from the resale market. Please refer to the following link for details on the eligibility to buy a HDB resale flat: http://www.hdb.gov.sg/fi10/fi10321p.nsf/w/BuyResaleFlatEligibilitytobuy. There is a five-year minimum occupation period before flat owners can sell their flats in the open market. In addition, with effect from August 2013, Singapore Permanent Resident households have to wait three years from the date of obtaining Singapore Permanent Resident status before they can buy a resale HDB flat. Foreigners are not allowed to purchase HDB flats.

[63] In 2012, about 34,800 private residential units with a value of about $52 billion were transacted; 2,900 commercial units with a value of about $5 billion were transacted and 5,000 industrial units with a value of about $7 billion were transacted (data excludes en bloc sales).

The primary role of estate agents and salespersons is to facilitate property transactions for their clients. For transactions involving salespersons, they would handle the initial stage of the property transaction, including marketing of the properties, bringing together buyers and sellers, negotiating the prices, and providing advice on policies and procedures relating to property transactions and financing. The salespersons' involvement in the property transactions would end after the buyer pays the option fee to purchase the property. Thereafter, the conclusion of the sale agreement and payment of stamp duties are facilitated by a conveyancing lawyer.

The development and sale of uncompleted private housing units are regulated under the Housing Developers (Control and Licensing) Act (HDCLA) administered by the Controller of Housing (COH). The HDCLA is intended to protect buyers who are buying uncompleted properties "off-plan". To this end, housing developers are required to follow standard procedures in the sale of the uncompleted units, e.g. use a standard Option to Purchase (OTP) and Sale and Purchase Agreement (S&PA).

ML/TF Risks

Compared to the tightly-controlled public housing segment and given the low turnover of non-residential sectors, the private housing segment may be relatively more susceptible to ML/TF. In 2012, there were about 34,800 transactions involving private housing units.

Given Singapore's inherent vulnerabilities due to our international financial hub status, visa-free travel for certain nationalities and large resident foreign presence, it is plausible that the real estate sector may be exploited for ML/TF purposes, especially by foreign elements seeking to move funds through Singapore. However, these risks are mitigated by the fact that it is not easy for them to hide their identities when making property purchases in Singapore.

For uncompleted private properties sold by developers, the purchaser is required to be clearly identified in the OTP and the S&PA. The purchaser is not allowed to use unidentified nominees to purchase a unit and the OTP cannot be assigned or transferred. There are also restrictions imposed on foreign ownership of residential land in Singapore. Such ownership is regulated by the Residential Property Act and a foreign person cannot acquire or purchase restricted residential properties (which include landed properties) unless prior approval of the Minister for Law is obtained for such purchases.

The majority of property transactions involve the engagement of services of salespersons either by the seller, buyer or both. However, the salesperson will only deal with a small fraction of the value of the property because the option fee, to be paid upfront to the property seller, only accounts for 1% to 5% of the total property price.

The larger value and less liquid nature of property and the measures put in place by the authorities make the real estate sector less attractive to potential terrorist financiers.

AML/CFT Controls

CEA was established in October 2010 under the EAA to strengthen regulatory oversight of the real estate agency sector. CEA's principal functions are to license estate agents and register salespersons, promote the integrity and competence of estate agents and salespersons through industry development, and engage in public education efforts to promote consumers' awareness of their rights and responsibilities in property transactions.

Estate agents and salespersons must adhere to the EAA in the conduct of their work. The EAA and its Regulations allow for enforcement actions to be taken against errant estate agents and salespersons, and the regulatory controls in place are a key risk mitigation measure. Additionally, there are two regulatory codes under the subsidiary legislation, namely, the Code of Ethics and Professional Client Care and the Code of Practice for Estate Agents which provide benchmarks for ethical behaviour and professional standards for estate agents and salespersons. Under the Code of Ethics and Professional Client Care, estate agents and salespersons are required to comply with all laws including statutory and regulatory requirements, and Practice Circulars and Guidelines issued by CEA. Infringement of the Codes and CEA's Practice Circulars and Guidelines can result in disciplinary action, including fines, suspension and/or revocation of licence or registration. In addition, if estate agents and salespersons commit offences under other laws during the course of their real estate agency work, CEA can also subject them to disciplinary action and consider reviewing the status of their licence or registration.

CEA issued the Practice Circular on the Prevention of Money Laundering and Countering the Financing of Terrorism ("the Circular") in November 2013 to estate agents and salespersons. The Circular covered obligations under Section 39 of the CDSA to file STRs with STRO, as well as the need to screen clients against UN lists of terrorists, terrorist organisations and other designated entities. CEA has also conducted outreach sessions to remind the industry on the relevant laws and obligations.

To ensure that estate agents and salespersons comply with the EAA and its Regulations, Guidelines and Codes, CEA plays a proactive role in monitoring industry operations. CEA has started to conduct compliance checks on estate agents. The scope of the compliance checks will be expanded in future to include compliance procedures related to AML/CFT.

The COH conducts regular checks on housing developers to ensure that sales of uncompleted properties are conducted in accordance with the requirements, e.g. proper identification of purchasers and non-assignment of the OTPs issued. The COH will continue to take appropriate steps to ensure that requirements in relation to the sale of uncompleted properties are complied with.

Next Steps

CEA's Practice Circular will be developed as a core Continuing Professional Development course to enhance AML/CFT training and awareness for the industry. It is a regulatory requirement for all registered salespersons to complete a minimum of six Continuing Professional Development credit hours a year to have their registration renewed.

CEA will be implementing the inspection framework for all estate agents to check on their compliance with the relevant AML/CFT obligations. Amendments to CEA's regulations will also be made in 2014 to increase the record keeping requirements for estate agents to five years to be consistent with the AML/CFT obligations.

The COH will continue to review the regulatory framework for the sale of uncompleted properties to ensure compliance with the relevant AML/CFT obligations.

Lawyers

Introduction

Lawyers in Singapore may act as both advocates and solicitors. They generally act for and provide legal advice to customers in conveyancing, litigation and corporate matters. At the end of 2012, there were approximately 4,300 lawyers, with a large proportion working in five of the biggest law firms in Singapore. Singapore lawyers have to be registered with and are governed by the Law Society of Singapore.

ML Risks

When acting for a corporate entity, lawyers are required to take reasonable measures to ascertain the identities of the natural persons who have a controlling interest in or exercise control over the corporate entity. A risk-based approach is adopted when deciding the measures to take. For example, lawyers are generally cautious about dealing with shell companies and will exercise enhanced CDD when there is doubt. Law practices are also obliged to conduct CDD checks if they receive cash payments above a prescribed amount.

Lawyers involved in the conveyance of properties in Singapore are prohibited from holding conveyancing money on behalf of their customers. Any conveyancing money received by a lawyer in connection with a conveyancing transaction must be placed with the Singapore Academy of Law or in an escrow account in accordance with an escrow agreement. Breach of this prohibition is a criminal offence which is punishable with a maximum of three years' imprisonment or a fine of up to $50,000 or both.

Lawyers may occasionally render trust advisory services. When a lawyer acts in his personal capacity as a trustee, he is required to have the necessary information needed to properly administer a trust. Lawyers involved in the administration of sophisticated trust arrangements generally use LTC service providers or business trusts, which are subjected to the necessary AML/CFT regulations in Singapore (please refer to the earlier section on LTCs).

In addition, lawyers have a statutory obligation to detect and report suspicious transactions except that they are not required to disclose information that is subject to legal privilege. Breach of this obligation to file STRs may result in criminal or disciplinary proceedings.

Due to the presence of strict controls, low incidences of cash acceptance and majority of the transactions being domestically-oriented, the ML risks for lawyers are relatively low in Singapore.

TF Risks

Although lawyers handle international transactions, these generally do not form a significant bulk of their work. Lawyers must ensure that they have enough information to determine the nature and purpose of the business relationship of a customer and the other party to the transaction for which the lawyer is instructed to act.

Similar to ML risks, lawyers are under a statutory obligation to detect and report suspicious transactions, including if they detect any risk or threat of TF. Breach of this obligation to file STRs may result in criminal or disciplinary proceedings. Hence, the TF risks in this sector are relatively lower.

AML/CFT Controls

Lawyers in Singapore are regulated under the Legal Profession Act (LPA) and subsidiary legislation promulgated pursuant to the LPA, which includes the Legal Profession (Professional Conduct) Rules ("the Rules"). The Rules are issued by the Law Society and are accompanied by the Law Society Council's Practice Direction 1 of 2008 on the Prevention of Money Laundering and the Funding of Terrorist Activities. The LPA and the Rules have the force of law, while the Practice Direction is legally enforceable.

These provide comprehensive AML/CFT measures, including the obligations to carry out CDD and record keeping, identify beneficial ownership, implement procedures and systems to identify customers who are PEPs, conduct ongoing CDD and apply enhanced CDD on higher risk customers, and to detect and report suspicious transactions. Lawyers are also expected to screen potential customers against the UN lists of terrorists, terrorist organisations and other designated entities before commencing a business relationship.

The Law Society of Singapore regularly inspects law practices to ensure compliance with the AML/CFT obligations. The Council may require a lawyer to produce documents, information or explanations required. On-site inspections are also carried out. Non-compliant lawyers will be subject to disciplinary action, with penalties ranging from fines or censures to being struck off the roll or suspension from practice.

Next Steps

In light of the revised FATF Recommendations, the obligations for lawyers to conduct CDD and to maintain records will be imported from the relevant subsidiary legislation into the LPA. The existing AML/CFT regulatory framework will also be reviewed and enhanced to be more consistent with international standards, and to mitigate any ML/TF risks identified.

There are also plans to increase industry outreach and promote continuing education on the applicable AML/CFT obligations, such as providing further guidance on circumstances requiring STRs to be filed.

Public Accountants and Other Professional Accountants

Introduction

In Singapore, professional accountancy services are mainly provided by public accountants or accounting entities owned and managed by public accountants. Public accountants are persons registered with and regulated by ACRA for the purpose of performing "public accountancy services", which are defined in the Accountants Act as the audit and reporting of financial statements and other such acts that are required by written law to be done by a public accountant. They are subjected to the requirements of the Accountants Act and the rules and standards prescribed under it[64]. All public accountants must also be members of the Institute of Singapore Chartered Accountants (ISCA) and adhere to its membership rules and standards. Public accountants provide services to the public through accounting corporations, limited liability partnerships, or firms i.e. partnerships and sole proprietorships ("accounting entities").

In addition to public accountants, professional accountancy services are also provided by professional accountants who are not registered as public accountants because they do not provide any public accountancy services. Many of them are members of professional bodies such as ISCA. Such professional accountants often work with public accountants to provide various accountancy related services.

Public accountants and professional accountants work in accounting entities, which can be broadly divided into two categories:

(i) Entities with publicly listed audit customers: about 20 accounting entities comprising four large accounting firms (about 40 public accountants in each firm), and about 16 medium-sized accounting entities (about five to 15 public accountants in each entity); and
(ii) Entities with no listed customers: about 600 small accounting entities with one or two public accountants in each entity ("small and medium practices").

While the customers and underlying transactions served by the accounting entities could be significant, the sector is relatively small in terms of size and share of economic activities. At the end of 2012, there were 995 public accountants working in 633 accounting entities.

ML Risks

Services provided by public accountants and professional accountants through accounting entities predominantly relate to audit, accounting and related services such as tax advisory. Some public accountants and professional accountants provide other services, such as setting up or managing companies or other legal persons, but they do so through separate entities that act as CSPs or business recovery/liquidators. Only a small proportion of services provided by public accountants and professional accountants are of the kind that could be exploited by those seeking to launder criminal proceeds, such as handling of customers' monies. Additionally, accounting entities do not handle customers' funds.

[64] In particular, public accountants should comply with the Singapore Standards on Auditing and Singapore Standard on Quality Control 1, and the Code of Professional Conduct and Ethics for Public Accountants and Accounting Entities, Fourth Schedule, Accountants (Public Accountants) Rules, Accountants Act.

TF Risks

The TF risks are minimal owing to the domestically-oriented nature of business for the accounting entities. As a relatively small proportion of their revenue is derived from exported services (23.9% in 2010), exposure to activities which might be used to aid TF is lower.

In addition, public accountants are required by the Code of Professional Conduct and Ethics and auditing standards to conduct CDD and not deal with customers who might jeopardise their integrity. As such, public accountants would have a relatively low percentage of customers who present a higher risk in this area.

AML/CFT Controls

Public accountants must adhere to the Code of Professional Conduct and Ethics prescribed under the Accountants Act ("the Code"), as well as auditing standards for their audit work. The Code is mandatory for all Public Accountants and failure to observe the Code may result in disciplinary action by ACRA under the Accountants Act. In addition, all ISCA members need to comply with requirements similar to those prescribed under the Code and non-compliance may result in disciplinary action by the ISCA. ISCA has also prescribed the Statement of Auditing Practice SAP 1 (formerly the SAP 19) – "Guidance to Auditors on Money Laundering and Terrorism Financing", which details public accountants' and ISCA members' requirements and obligations in this area.

The Code has two requirements relevant to the integrity of customers and source of customers' funds. Firstly, it requires public accountants to undertake professional appointment and customer acceptance procedures, which include the assessment of customer involvement in illegal activities such as ML[65]. Public accountants should decline to enter the customer relationship if such issues are known. Secondly, public accountants must make appropriate enquiries about the source of customer assets to check whether they were derived from illegal activities.

Accounting entities generally have monitoring in place to ensure that they meet the standards and requirements. As auditors, public accountants are required by the auditing standards to give reasonable assurance about the truth and fairness of financial statements, including by establishing the authenticity of the underlying transactions to ensure, among other things, that their audit customer's transactions are not fronts for illicit activities. Accounting entities generally have processes in place to monitor for unusual and/or suspicious transactions and file STRs.

In addition, public accountants are also subjected to a rigorous auditor oversight regime, the Practice Monitoring Review Programme which is administered by ACRA, to ensure that they adhere to the auditing standards. ACRA inspects the quality controls, including customer acceptance, of accounting firms that audit publicly listed entities through the Practice Monitoring Review Programme.

In addition to the AML/CFT controls in place, larger accounting entities, which have more international customers and higher volume of non-audit services, subscribe to and use third-party customer screening databases to ensure that they do not deal with UN listed terrorists, terrorist organisations and other designated entities.

[65] Please refer to paragraphs 210.1 to 210.6 of the Code.

Next Steps

ISCA is updating SAP 1 in 2014 to ensure that the guidance is up-to-date with the latest requirements and practices. This will also be a good opportunity to remind the accountancy profession of its obligations and provide guidance on how to successfully apply a risk-based AML/CFT controls regime.

Another area that may be strengthened is monitoring and enforcement to ensure that the requirements are implemented robustly, including when public accountants engage in non-traditional services beyond auditing which may present ML/TF risks. In Singapore, public accountants' audit work is inspected by ACRA, with the assistance of ISCA in the case of small and medium practices. However, these inspections do not cover non-audit work. There is also a need to ensure that professional accountants who are not public accountants implement the requirements and best practices appropriately. As in most other jurisdictions, aside from auditing services, Singapore's professional accountants are self-regulated through professional bodies that have to play a role in strengthening the profession's ability to mitigate ML/TF risks. However, these inspections do not cover non-audit work. ACRA will be working with the profession to consider how AML/CFT supervision can be further improved.

Non-Profit Organisations

Charities

At the end of 2012, there were 2,130 charities[66] in Singapore, of which 580 were Institutions of a Public Character (IPCs)[67]. The majority of the charities and IPCs do not receive large sums of donations. Based on latest available statistics, only 6% of the charities have annual receipts exceeding $10 million. These are mainly the higher education institutions, health institutions and the larger voluntary welfare organisations and religious organisations (other than mosques) which are generally domestically oriented.

Charities are regulated by the Office of the Commissioner of Charities (COC). They are required to submit their annual reports and financial statements which have to be audited or reviewed by external auditors or independent examiners. All charities in Singapore must be registered and meet the following conditions under the Charities Act:

(i) The institution must have at least three governing board members, of whom at least two must be Singapore Citizens or Permanent Residents; and
(ii) The purposes/objectives of the institution must be beneficial, wholly or substantially, to the community in Singapore.

[66] As defined under case law, a charity must be set up exclusively for charitable objects (such as relief of poverty, advancement of education or religion, and other purposes beneficial to the community). The activities carried out must benefit the public at large.

[67] IPC is a status conferred to registered charities. Charities with this status are allowed to issue tax deductible receipts for donations made to them. The activities carried out have to be exclusively beneficial to the community in Singapore as a whole and not be confined to sectional interests or groups of persons based on race, belief or religion.

A permit from the Office of the COC is required before anyone can conduct a fund-raising appeal for foreign charitable purposes or overseas beneficiaries. The permit is granted on the condition that at least 80% of the net proceeds of the funds raised have to be applied towards charitable purposes within Singapore, unless the COC allows otherwise. Permit holders are required to provide accurate information to donors and use the donations in accordance with the specified intention. They are also required to maintain proper accounting records. Permit holders will need to submit a set of audited statement of accounts within 60 days after the last day of the fund-raising appeal. The COC also has the power to issue a prohibition order to stop any party from carrying out the fund-raising appeal if he is satisfied that: (i) it has not been conducted in good faith; (ii) the persons conducting it are not fit and proper to do so; or (iii) it is not in public interest.

Mosques

Mosques in Singapore are regulated by Majlis Ugama Islam Singapura (MUIS), a statutory board formed by an Act of Parliament - the Administration of Muslim Law Act (AMLA), and reports to the Minister-in-Charge of Muslim Affairs. Under AMLA, all mosques are administered by MUIS.

MUIS appoints Muslim community leaders to the Mosque Management Boards (MMB) to manage the mosque operations on a two year term. The appointed MMBs manage the mosque operations in accordance with the Mosque Management and Financial Regulations issued by MUIS. The MMBs are provided with training on the regulations so as to ensure that they understand and are able to comply with the regulations issued.

Since 2005, MUIS has formed a Mosque Shared Financial Services unit. The unit is recruited and appointed by MUIS to work with each mosque to prepare their financial statements on a timely basis on a shared accounting system. With the formation of the unit, the mosques and MUIS are better able to manage their financial resources. Each mosque is subject to an external audit by an auditor (public accountant) appointed by MUIS under the Second Schedule of the AMLA.

Mosque building and operations are almost exclusively funded locally via mechanisms such as the Mosque Building and Mendaki Fund[68], Friday and Chest Collections, fees for religious classes and services, and local fund-raising projects such as the selling of cooked food. For national fund-raising via the media, mosques would need to apply for a licence from MUIS. In instances where there are overseas donations offered to mosques, the funds are channelled through MUIS to monitor such donations and their sources. This is a requirement stipulated in the Mosque Financial Regulations issued by MUIS.

Overall

Singapore's NPO sector is generally domestically-oriented and not large. There are ample safeguards in place to ensure that funds raised are not misused, and these help to deter the abuse of this sector for ML/TF. To ensure that the ML/TF risks in this sector remain low, outreach efforts on AML/CFT issues will continue to be made to the sector where necessary.

[68] A monthly payroll deduction programme collected via the Central Provident Fund Board.

Risks to Study Further

Precious Stones and Metals Dealers

The precious stones and metals dealers sector is a varied and segmented sector without a specific regulatory or licensing body. Industry associations such as the Singapore Jeweller Association and Diamond Exchange have limited reach to the industry itself.

Based on preliminary feedback from the industry, most transactions are geared towards personal consumption rather than for trading purposes. Nonetheless, we have noted instances where Singapore had hosted diamond trade shows, and there could be some plans to grow the precious metals industry. The ML/TF risks will have to be analysed further.

While there are international typologies on the use of precious stones and metals as a tool to launder money, particularly as a store-of-value to move illicit proceeds easily, there have been very few cases of ML and no case of TF involving this sector to date.

The Singapore Freeport

The Singapore Freeport, opened in May 2010, is a secured storage facility for high-value collectibles, such as art pieces, wine, and precious metals. Long-term storage and trade of high-value collectibles brought in from outside Singapore, are carried out within the Singapore Freeport without attracting any duties or Goods and Services Tax. The Singapore Freeport is within Singapore's customs territory and is not a free trade zone.

Singapore Freeport's licensees are assessed under the TradeFIRST[69] framework, based on a range of criteria covering inventory management and controls, compliance records, and security measures. For instance, the licensees are required to ensure strict controls over the physical movement of goods, vehicles and people entering or exiting the Singapore Freeport.

Singapore Customs re-assesses the licensees every one, two or three years, depending on their compliance or risk rating under the TradeFIRST framework. The re-assessment is to ensure that the licensees maintain the standard that each individual band requires and their internal processes and standard operating procedures are accurate and up-to-date. Singapore Customs also has the right to re-assess the licensees anytime within the validity period of the licence, especially if they have a poor compliance record. The penalties for breaches by the licensees include the requirement to lodge a bank guarantee every year (vis-à-vis lodging a bank guarantee once every three years) and the revocation of the licences.

Licensees of the Singapore Freeport are granted simplified customs declaration for the storage of goods within, but they are required to put in place a robust inventory system to track the movement of these goods. They are also responsible to keep records of all supporting documents for at least five years and show them to Singapore Customs when required. In addition, Singapore Customs has the powers to enter all the locations within the Singapore Freeport to conduct checks and perform investigation.

The licencees are also subject to domestic AML/CFT laws and regulations and are mandated to detect and report suspicious transactions to STRO.

Singapore will study the ML/TF risks in these two areas further, and consider implementing appropriate mitigation measures. In the interim, STRO will also continue to conduct outreach to the relevant sectors to educate the stakeholders of the ML/TF threats and typologies and highlight to them their STR reporting obligations.

[69] TradeFIRST (Trade Facilitation & Integrated Risk-based SysTem) is an integrated assessment framework that provides a holistic assessment of a company to support Singapore Customs in its trade facilitation and compliance efforts.

Annexes

ANNEX A - Case Studies

(i) ML Domestic Threats – Case Study on Cheating

Case of Public Prosecutor vs. Koh Seah Wee and others

In 2007, Koh Seah Wee was appointed the Deputy Director of the Technology and Infrastructure Department of the Information Technology Division of the Singapore Land Authority (SLA), a position that allowed him to approve purchases valued up to $60,000.

Koh and his subordinate, Lim Chai Meng, conspired with private sector contractors to cheat SLA by awarding contracts to these contractors for the supply of information technology goods and services which SLA did not need. The contractors had no intention of fulfilling these contracts.

When SLA paid the contractors, they transferred most of the payments to Koh and Lim. Over a three year period, SLA was deceived into paying about $12 million for goods and services it did not receive.

Koh was charged with more than 300 counts of cheating and ML offences. He was sentenced to 22 years' imprisonment. Lim was charged with 282 counts of cheating and sentenced to 15 years in jail. Investigators also seized and forfeited a total of:

(i) $6.2 million worth of properties and cash, luxury watches and jewellery from Koh and $1.3 million from Koh's wife; and
(ii) $1.2 million worth of assets and valuables, including luxury watches and $2 million from Lim's close relatives.

The vendors who conspired with them to commit the fraud against SLA were also sentenced to between 18 months and 10 years imprisonment.

(ii) ML Domestic Threats – Case Study on Criminal Breach of Trust

Case of Public Prosecutor vs. Matthew Yeo Kay Keng

Over a period of two years, Matthew Yeo Kay Keng, aged 35, an account manager, siphoned around $2 million from a telecommunications company by selling stolen phones to third parties.

Between 2008 and 2010, Yeo misappropriated 3,085 handphone sets. He created fictitious subscription contracts for mobile services supposedly for corporate customers. He would then sell off the handphone sets bundled with subscription contracts at close to retail prices to resellers for cash, on the pretext of personally delivering the handphones directly to the customers. He deposited a portion of the criminal proceeds into his personal bank account.

Yeo spent his criminal proceeds on luxury watches, luxury cars and other investments. He was jailed for a total of six years for CBT and ML.

(iii) ML Foreign Threats – Case Study on Cheating Involving a Shell Company

Case of Public Prosecutor vs. Jay Alan Thierens

Jay Alan Thierens, a United Kingdom national, incorporated Fairwind Pte Ltd in Singapore through a CSP and opened bank accounts in Singapore in the name of Fairwind. Investigations revealed that an account of Fairwind received monies from victims of investment scams. The victims, residing in various jurisdictions, received cold calls from an individual, purporting to offer exclusive pre-initial-public offering shares of foreign companies with the promise of attractive returns. They then received invoices via email with instructions to remit funds to various overseas bank accounts, including the said account of Fairwind in Singapore.

The funds deposited by the victims into Fairwind's account were remitted overseas soon after they were received. From June to September 2011, Fairwind's account received more than EUR 400,000 while more than EUR 350,000 was remitted out of the same account during the same period. These transactions were not consistent with Fairwind's registered business activity of building and repairing pleasure crafts, lighters and boats, and general wholesale trade.

As this case involved various jurisdictions, CAD collaborated closely with its foreign counterparts to exchange information, which was very useful in furthering the investigation.

On 16 December 2011, Thierens was convicted of criminal offences and sentenced to a total of 15 months' imprisonment.

(iv) ML Foreign Threats – Case Study on Money Mules

Cases of Public Prosecutor vs. Nigam Kok Min and Public Prosecutor vs. Diana Chua

Ngiam Kok Min, aged 45, an odd job worker, allowed his bank accounts to receive fraudulent payments from victims of fraud overseas.

In April 2012, Ngiam was approached by Chua Gek Choo Dianna Nicole, aged 43, to open bank accounts in Singapore in order to receive monies from overseas. Ngiam was promised a 3% commission for the work. Thereafter, he received a large sum of monies (totalling $1,249,829.23) from eight overseas remitters and subsequently passed the withdrawn monies (totalling $850,000.00) personally to Chua, on six occasions. Despite his suspicions about her requests, Ngiam proceeded to take part in the transactions. In total, he received a sum of $10,451.94 for his work.

On separate occasions, Chua also received two fraudulent transactions of $126,420.00 on 9 December 2011 and $172,971.40 on 26 April 2012. In total, she received $43,991.50 for her work.

Investigations revealed that the overseas remitters and their banks were victims of fraudulent email instructions. The banks were deceived into remitting payments from their customers' accounts into Chua's and Ngiam's accounts after receiving email instructions, purportedly from their customers.

Ngiam was sentenced on 15 October 2012 to a total of 54 months' imprisonment for criminal offences. Chua was sentenced on 19 July 2013 to a total of 36 months' imprisonment for criminal offences.

The successful conviction would not have been possible without close cooperation between CAD and its foreign counterparts. The exchange of information between authorities helped to verify existing information and provided new leads for the investigation.

ANNEX B - Singapore Regulatory Instruments

The Singapore Government issues various regulatory instruments in carrying out its functions. These include the following which have been cited in this report.

Acts

Acts contain statutory laws which are passed by Parliament. These have the force of law and are published in the Government Gazette. Examples cited include the Banking Act and the CDSA.

Subsidiary Legislation

Subsidiary legislation is issued under the authority of the relevant Acts and typically fleshes out the provisions of an Act and spells out in greater detail the requirements that the regulated entities or other specified persons have to adhere to. Subsidiary legislation has the force of law and may specify that a contravention is a criminal offence. They are also published in the Government Gazette. Examples in this report are the Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009 and the Legal Profession (Professional Conduct) Rules.

Directions and Notices

Directions detail specific instructions to regulated entities or other specified persons to ensure compliance. They could take the form of Directives or Notices. Like subsidiary legislation, they have force of law and may specify that a contravention is a criminal offence. Examples in this report are the CRA Direction 146/1/2 Customer Due Diligence Measures (1267 List) and the MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism.

Guidelines

Guidelines set out principles or "best practice standards" that govern the conduct of specified entities or persons. While contravention of guidelines is not a criminal offence and does not attract civil penalties, specified entities or persons are encouraged to observe the spirit of these guidelines. An example in this report is the MAS' Guidelines for the Operations of Wholesale Banks.

Practice Notes

Practice Notes are meant to guide specified institutions or persons on administrative procedures relating to, among others, licensing, reporting and compliance matters. Contravention of a practice note is not a criminal offence, unless a procedure stated in the Practice Note is also required by an Act or Regulation. An example of an enforceable Practice Note in this report is the Law Society of Singapore Council's Practice Direction 1 of 2008 on the Prevention of Money Laundering and the Funding of Terrorist Activities.

Circulars

Circulars are documents which are sent to specified persons for their information or are published on the relevant government agency's website to guide the activities of the specified persons. Depending on the source for the circulars, they could be enforceable in cases of breach of the requirements of the circulars. An example of an enforceable circular in this report is CEA's Practice Circular on the Prevention of Money Laundering and Countering the Financing of Terrorism.

Annexes

ANNEX C - List of Abbreviations

ACRA	Accounting and Corporate Regulatory Authority
ACU	Asian Currency Unit
AGC	Attorney-General's Chambers
AML	Anti-Money Laundering
AMLA	Administration of Muslim Law Act
APEC	Asia-Pacific Economic Cooperation
APG	Asia/Pacific Group on Money Laundering
ASEAN	Association of Southeast Asian Nations
ASEM	Asia-Europe Meeting
CAD	Commercial Affairs Department
CBNI	Cash or Bearer Negotiable Instrument
CBT	Criminal Breach of Trust
CDD	Customer Due Diligence
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
CEA	Council for Estate Agencies
CF	Corporate Finance
CFT	Countering the Financing of Terrorism
CMR	Cash Movement Report
CMS	Capital Markets Services
CNB	Central Narcotics Bureau
COC	Commissioner of Charities
COH	Controller of Housing

Annexes

CPC	Criminal Procedure Code
CPIB	Corrupt Practices Investigation Bureau
CRA	Casino Regulatory Authority
CSP	Corporate Service Provider
CT	Counter Terrorism
CU	Charities Unit
DL insurers	Direct life and composite insurers
DNFBP	Designated Non-Financial Business and Profession
EAA	Estate Agents Act
EOI	Exchange of Information
FA	Financial Adviser
FATF	Financial Action Task Force
FI	Financial Institution
FIG	Financial Investigation Group, Commercial Affairs Department
FIU	Financial Intelligence Unit
FMC	Fund Management Company
FTZ	Free Trade Zone
GDP	Gross Domestic Product
HDCLA	Housing Developers (Control & Licensing) Act
IA	Insurance Act
IB	Insurance Broker
ICA	Immigration & Checkpoints Authority
IMA	International Market Agent

IMC-EC	Inter-Ministry Committee for Export Control
IMC-TD	Inter-Ministry Committee on Terrorist Designation
INTERPOL	International Criminal Police Organisation
IPC	Institution of a Public Character
IPTO	Insolvency and Public Trustee's Office
IRAS	Inland Revenue Authority of Singapore
IR	Integrated Resort
ISCA	Institute of Singapore Chartered Accountants
ISD	Internal Security Department
ISP	Industry Sound Practices
JI	Jemaah Islamiyah
LEA	Law Enforcement Authority
LPA	Legal Profession Act
LTC	Licensed Trust Company
MACMA	Mutual Assistance in Criminal Matters Act
MAS	Monetary Authority of Singapore
MCRB	Money-changing and Remittance Businesses
MHA	Ministry of Home Affairs
MinLaw	Ministry of Law
ML	Money Laundering
MLA	Mutual Legal Assistance
MMB	Mosque Management Board
MMOU	Multilateral Memorandum of Understanding

MOF	Ministry of Finance
MOU	Memorandum of Understanding
MSF	Ministry of Social and Family Development
MUIS	Majlis Ugama Islam Singapura
NPO	Non-Profit Organisation
NRA	National Risk Assessment
OECD	Organisation for Economic Cooperation and Development
OTP	Option to Purchase
PBIG	Private Banking Industry Group
PCA	Prevention of Corruption Act
PCG	Police Coast Guard
PEP	Politically Exposed Person
PMFTR	Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009
PS(O)A	Payment Systems (Oversight) Act
QFB	Qualifying Full Bank
S&PA	Sale and Purchase Agreement
SAP	Statement of Auditing Practice
SFA	Securities and Futures Act
SLA	Singapore Land Authority
SOP	Standard Operating Procedure
SPF	Singapore Police Force
STA	Singapore Trustees Association
STR	Suspicious Transaction Report

STRO	Suspicious Transaction Reporting Office
SVF	Stored Value Facility
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCA	Trust Companies Act
TF	Terrorist Financing
TSOFA	Terrorism (Suppression of Financing) Act
UML	Unlicensed Moneylending
UN	United Nations
UNSCR	United Nations Security Council Resolution
URA	Urban Redevelopment Authority

ISBN 978-987-07-8812-4

Published in January 2014

Ministry of Home Affairs
New Phoenix Park,
28 Irrawaddy Road,
Singapore 329560
www.mha.gov.sg

Ministry of Finance
100 High Street,
#06-03 The Treasury,
Singapore 179434
www.mof.gov.sg

Monetary Authority of Singapore
10 Shenton Way,
MAS Building,
Singapore 079117
www.mas.gov.sg