

**MONEY LAUNDERING
RISK ASSESSMENT REPORT
SINGAPORE
2024**

Contents

TABLE OF ACRONYMS.....	3
1. FOREWORD	6
2. OBJECTIVE	7
3. EXECUTIVE SUMMARY	8
4. INTRODUCTION TO SINGAPORE	12
5. ML NRA METHODOLOGY	22
6. MONEY LAUNDERING THREAT.....	24
7. SECTORAL RISK ASSESSMENTS – FINANCIAL SECTOR.....	51
8. SECTORAL RISK ASSESSMENTS – DNFBP SECTOR	95
9. CONCLUSION.....	124
ANNEX – SINGAPORE’S FREE TRADE ZONE REGIME	125

TABLE OF ACRONYMS

ABS	The Association of Banks in Singapore
ABSD	Additional Buyer's Stamp Duty
ACD	AML/CFT Division of the Ministry of Law
ACCESS	Association of Cryptocurrency Enterprises and Start-Ups, Singapore
ACIP	Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership
ACPN	Anti-Corruption Partnership Network
APPACT	Alliance of Public Private Cybercrime Stakeholders
ACRA	Accounting and Corporate Regulatory Authority
AFP	Australian Federal Police
AGC	Attorney-General's Chambers
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
AML/CFT SC	Anti-Money Laundering, Countering the Financing of Terrorism Steering Committee
APG	Asia/Pacific Group on Money Laundering
ARIN-AP	Asset Recovery Inter-Agency Network Asia Pacific
ASC	Anti-Scam Centre
ASCom	Anti-Scam Command
ATM	Automated Teller Machine
BEC	Business E-mail Compromise
BO	Beneficial Ownership
CAD	Commercial Affairs Department of the Singapore Police Force Singapore's Financial Intelligence Unit, the Suspicious Transaction Reporting Office, is part of CAD.
CBT	Criminal Breach of Trust
CCA	Casino Control Act
CCR	Casino Control Regulations
CCTV	Closed-Circuit Television
CDD	Customer Due Diligence
CDP	Central Depository
CDSA	Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
CEA	Council for Estate Agencies
CITES	International Consortium on Combatting Wildlife Crime
CMA	Computer Misuse Act
CNB	Central Narcotics Bureau
COH	Controller of Housing
CPIB	Corrupt Practices Investigation Bureau
CRA	Casino Regulatory Authority
CRS	Common Reporting Standard
CSA	Cyber Security Agency of Singapore
CSIS	Chartered Secretaries Institute of Singapore
CSP	Corporate Service Provider
CTR	Cash Transaction Report
DPRK	Democratic People's Republic of Korea
DPT	Digital Payment Token
DNFBPs	Designated Non-Financial Businesses and Professionals

EAA	Estate Agents Act
EAM	External Asset Manager
Egmont	Egmont Group of Financial Intelligence Units
ECDD	Enhanced Customer Due Diligence
EP 200	Ethics Pronouncement 200
eTRS	Electronic Tourist Refund Scheme
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FMC	Fund Management Company
FSMA	Financial Services and Markets Act
FTZ	Free Trade Zone
GDP	Gross Domestic Product
GST	Goods and Services Tax
HDCLA	Housing Developers (Control and Licensing) Act
HNWI	High Net Worth Individual
IACCC	International Anti-Corruption Coordination Centre
ICC	Internal Controls Code
ICO	Initial Coin Offering
IMA	International Market Agent
IMCS	Inter-Ministry Committee on Scams
IMF	International Monetary Fund
IPTO	Insolvency and Public Trustee's Office
IRAS	Inland Revenue Authority of Singapore
ISCA	Institute of Singapore Chartered Accountants
ISTRA	Inter-Agency Suspicious Transaction Report Analytics Taskforce
IT	Information Technology
KEO	Key Executive Officer
Law Society	The Law Society of Singapore
LEA	Law Enforcement Agency
LLP	Limited Liability Partnership
LTC	Licensed Trust Company
MACMA	Mutual Assistance in Criminal Matters Act
MAS	Monetary Authority of Singapore
MHA	Ministry of Home Affairs
Minlaw	Ministry of Law
ML	Money Laundering
MLA	Mutual Legal Assistance
MOF	Ministry of Finance
MTF	Missing Trader Fraud
NBCC	Non-Bank Credit Cards
NRA	National Risk Assessment
OCA	Organised Crime Act
OPT	Option to Purchase
PBA	Pawnbrokers Act 2015
PEP	Politically Exposed Person
PF	Proliferation Financing
PMTFPFR	Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules

PS Act	Payment Services Act
PSMD	Precious Stones and Precious Metals Dealers
PSPM	Precious Stones, Precious Metals and/or Precious Products
PSPM Act	Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act
RBA	Risk-Based Approach
RFA	Registered Filing Agent
RQI	Registered Qualified Individual
RTIG	Risks and Typologies Inter-Agency Group
S&PA	Sales & Purchase Agreement
SFA	Securities and Futures Act
Singpass	Singapore Personal Access
SME	Small and Medium-sized Enterprise
SPF	Singapore Police Force
STR	Suspicious Transaction Report
STRO	Suspicious Transaction Reporting Office
SONAR	STRO Online Notices and Reporting Platform
TBML	Trade-Based Money Laundering
TF	Terrorism Financing
TT	Telegraphic Transfer
UML	Unlicensed Moneylending
UNODC	United Nations Office of Drugs and Crime
US	United States of America
VASP	Virtual Assets Service Provider
VCC	Variable Capital Company
WOG	Whole-of-Government

1. FOREWORD











- 1.1 As an international business, financial and trading centre, Singapore is exposed to the risks of transnational Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF). Criminals will seek to exploit our economic openness, financial system, and business infrastructure to move funds and assets. Hence it is important that Singapore remain vigilant to the risks of being misused for illicit funds and asset flows.
- 1.2 The ML/TF/PF risks that Singapore is exposed to have become more complex, due to the global geo-political climate and macro-economic events, and the increased use of sophisticated financial and business structures. Technological advancements have also provided additional channels for criminals to launder or move their illicit funds and assets across jurisdictions, with speed and ease. These developments are taken into consideration in this ML National Risk Assessment (NRA).
- 1.3 The fast-changing threat landscape has profound impact on how our authorities cooperate and coordinate with each other, and work with the private sector to detect and mitigate ML risks. International collaboration and cooperation are also crucial to deal with the increasingly complex nature of funds and asset flows across borders.
- 1.4 Singapore strives to continuously improve our anti-money laundering (AML), countering the financing of terrorism (CFT) and counter proliferation financing (CPF) regime. Our regime is aligned with international standards and best practices, grounded in robust and comprehensive laws and regulations, rigorous and risk-focused supervision, and effective enforcement and prosecution. Significant steps have been taken recently to strengthen our AML/CFT/CPF regime including in our legal and regulatory framework, inter-agency cooperation, usage of financial intelligence, risk-based supervision and risk surveillance, public-private partnerships, enforcement, prosecution, and asset recovery, as well as international cooperation.
- 1.5 Singapore is an active member of the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG) and held the FATF Presidency for the term July 2022 to June 2024. We also contribute actively to the work of other international financial crime fighting bodies, such as the Egmont Group and INTERPOL.
- 1.6 Our overall AML/CFT/CPF efforts are guided by the AML/CFT Steering Committee (AML/CFT SC), co-chaired by the Permanent Secretary of the Ministry of Home Affairs (MHA), the Permanent Secretary of the Ministry of Finance (MOF) and the Managing Director of the Monetary Authority of Singapore (MAS). The AML/CFT SC sets Singapore's policy objectives and directions for combating ML, TF and PF. The senior level involvement and significant resources invested into AML/CFT work in Singapore demonstrate Singapore's strong commitment towards combatting ML, TF and PF. This NRA, developed under the auspices and with the guidance of the AML/CFT SC, provides a consolidated view of Singapore's understanding and assessment of the prevailing and emerging ML threats and vulnerabilities that Singapore and the various sectors face, as well as the level of controls within each sector. The findings from this NRA support Singapore's and its agencies' prioritisation of key risks and the application of supervisory, enforcement and mitigation measures.

2. OBJECTIVE

- 2.1 This NRA provides an overview of Singapore's key ML risks, which synthesises Singapore's observations arising from the work of the Risk and Typologies Inter-Agency Group (RTIG), risk assessments conducted by agencies, and information from various other sources. The NRA provides law enforcement agencies (LEAs), regulators, supervisors, and industry players with a consolidated picture of the key national ML risks and vulnerabilities, allowing them to adopt a more targeted and focused approach towards the development and implementation of Singapore's national AML strategies and policies and their own AML defences.
- 2.2 This NRA provides:
- (i) An introduction to Singapore;
 - (ii) An overview of key ML threats impacting Singapore;
 - (iii) Sectoral risk assessments of the financial sector; and
 - (iv) Sectoral risk assessments of the Designated Non-Financial Businesses and Professions (DNFBP) sectors.
- 2.3 This NRA will be followed by the publication of Singapore's National AML Strategy, which will provide a roadmap of the actions which Singapore has taken and will be taking to further strengthen our AML regime, and address the threats and vulnerabilities observed.
- 2.4 To complement this NRA and to provide a deeper dive into identified key risk areas, Singapore is also updating our risk assessments relating to proliferation financing, misuse of legal persons, virtual assets, and legal arrangements. Singapore has also recently published a risk assessment on environmental crime ML to raise awareness and outline mitigation measures to address the risks observed in this emerging area.
- 2.5 Financial institutions (FIs) and DNFBPs should refer to the findings in this NRA to assist them in their risk assessments and implementation of risk mitigation. FIs and DNFBPs should also continue to take into account other relevant risk assessments and guidance that are issued by the authorities when reviewing this NRA.

3. EXECUTIVE SUMMARY

- 3.1 This NRA reflects Singapore's updated understanding of its key ML threats and risks. It consolidates observations from our ongoing monitoring and surveillance by all relevant supervisory, law enforcement and policy agencies, and financial intelligence unit, and our engagements with the private sector. It also incorporates inputs from Singapore's key¹ foreign law enforcement and financial intelligence partners, which allow us to better evaluate our foreign ML threats.
- 3.2 In determining the key ML threats and risks to Singapore, an extensive range of qualitative and quantitative threats, vulnerabilities and control factors was considered. Overall, Singapore's key ML threats arise from a range of predicate offences, as criminals seek to exploit Singapore's political and economic stability, strong rule of law, infrastructure, and wide range of services that our financial and other sectors provide. Taking into account a range of indicators, including observations and cases from law enforcement and financial intelligence, international cooperation requests and feedback from foreign counterparts, and international typologies, Singapore's key ML threats are fraud (particularly, cyber-enabled fraud), organised crime, corruption, tax crimes, and trade-based money laundering. The banking (including wealth management sector) is assessed to pose the highest ML risks to Singapore. Among the DNFBP sectors, corporate service providers (CSPs) pose higher ML risks given the role they play in providing upstream services such as incorporation of companies.
- 3.3 The key findings of the NRA are summarised in the table below.

KEY ML THREATS	
 Fraud, <i>particularly cyber-enabled fraud</i>	 Corruption, <i>originating from abroad</i>
 Organised Crime, <i>especially illegal online gambling associated with foreign organised criminal groups</i>	 Tax Crimes, <i>originating from abroad</i>
	 Trade-based money laundering
OTHER NOTABLE ML THREATS	
 Environmental Crime	 Drug-related offences
 Cyber-crime	
HIGHER ML RISK SECTORS	
<i>Inherent exposure to key ML threats, and cross-border transactions/customers, despite stronger controls</i>	
 Banks pose highest ML risks to Singapore	
 <i>Abused through their roles as professional / financial intermediaries, exposure to cross-border transactions, and/or placement in high value assets, while taking into account controls in place</i>	
<ul style="list-style-type: none"> • Corporate Services Providers • Real Estate • Casinos • Licensed Trust Companies • Precious stones and precious metal dealers 	
<ul style="list-style-type: none"> • Digital Payment Token Services Providers • Payment Institutions, with cross border money transfer services • External Asset Managers 	

¹ Including all Financial Action Task Force and Association of Southeast Asian Nation members.

- 3.4 **Key ML threats.** As an international business, financial and trading centre, Singapore is exposed to external threats arising from predicate offences that have a foreign nexus. **Notably, Singapore LEAs see a high number of ML cases arising from foreign fraud, particularly cyber-enabled fraud².** Fraud is also the most frequently cited offence in foreign authorities' requests to Singapore for assistance, through both the Suspicious Transaction Reporting Office (STRO) and LEAs. It is also increasingly a key crime of concern globally. Authorities have observed that fraudulent proceeds are often professionally laundered and facilitated through third parties, such as multiple layers of corporate and individual mules and nominees, as well as through the financial and DNFBP sectors. In addition, Singapore's engagements with other jurisdictions have identified fraud to be the top predicate crime of concern posing an ML threat to Singapore.
- 3.5 **Over the years, Singapore has also observed an increase in ML threat posed by cyber-enabled fraud committed domestically, orchestrated by syndicates typically located overseas.** STRO and LEAs in Singapore note the abuse of mule networks, and the use of nominees in these well-orchestrated arrangements. This threat has been exacerbated by advancements in digitalisation, which allow syndicates to broaden their reach to the mass public through the abuse of social media platforms and transcend borders to launder their ill-gotten gains. Recognising that ML threats posed by cyber-enabled fraud is a global problem, Singapore, together with INTERPOL and the Egmont Group, led the development of the Report on Illicit Financial Flows from Cyber-Enabled Fraud issued by FATF, to share effective strategies to combat this threat.
- 3.6 **Another key ML threat faced by Singapore arises from foreign organised crime, and in particular illegal online gambling.** In the recent money laundering case, which involved over S\$3b worth of seized and prohibited assets, several of the accused persons were convicted of laundering proceeds which were suspected of being the benefits of illegal online gambling from foreign organised criminal groups. Some of these monies were held in bank accounts in Singapore. Others were converted into assets such as real estate, cars, handbags and collectibles. Aside from banks, other sectors were involved in the offenders' management of their assets (for instance, they had engaged CSPs to incorporate companies in Singapore through which they held their assets, purchased properties through real estate salespersons, and placed their funds in other high value goods through precious stones and precious metals dealers).
- 3.7 Further, in line with global trends, LEAs have observed an increase in the layering of illicit funds across multiple jurisdictions, as organised crime groups and professional money launderers become more sophisticated in their laundering techniques. LEAs have consequently noted that foreign authorities have often identified ML as the key offence (as opposed to other serious offences) in requests for assistance. In this regard, **STRO and LEAs have also observed criminal proceeds arising from corruption, tax, and trade-based money laundering being layered through our jurisdiction (e.g. through shell/front companies and to a lesser extent trusts), before being transferred to other jurisdictions within a short span of time – making international cooperation even more important.**

² Cyber-enabled fraud is defined as fraud that is enabled through or conducted in the cyber environment and that (i) involves transnational criminality such as transnational actors and funds flows and (ii) involves deceptive social engineering techniques (see also FATF report on Illicit Financial Flows from Cyber Enabled Fraud, November 2023).

- (i) **Corruption** – The threat of corruption proceeds being laundered through our region is assessed to be high, given Singapore’s geographical location and status as an international business, financial and trading centre. This is also a priority risk area which the FATF Ministers have noted in April 2022, and asked the international community to remain vigilant to. Corruption is the third highest offence cited in incoming foreign requests to Singapore, with a large proportion of requests made via formal channels. The laundering of foreign corrupt proceeds in Singapore has been observed to involve a mix of self and third-party laundering, which may be facilitated by intermediaries such as banks and using legal persons. There were also instances where foreign corruption proceeds were converted into real estate.
- (ii) **Tax crimes** - As a wealth management hub, Singapore is inherently exposed to ML involving tax crime proceeds originating from abroad. Singapore has seen an increase in the number of incoming foreign requests relating to tax offences, via mechanisms such as mutual legal assistance (MLAs), and requests via STRO and INTERPOL. LEAs have also observed that legal persons and arrangements play a role in the laundering of foreign tax crime proceeds, where complex ownership and control structures could be used to hold funds and assets via bank accounts and other products. Intermediaries such as trust and company service providers, as well as asset managers may also be misused.
- (iii) **Trade-based money laundering (TBML)** - Given Singapore’s status as a trading and transportation hub, including for transshipment, Singapore faces an inherent threat of foreign TBML³. In recent years, Singapore has seen an increase in the number of requests from its foreign counterparts relating to TBML activities with a Singapore nexus. These cases may involve techniques such as over and under invoicing of goods and services and utilising financial and professional intermediaries.

3.8 Other notable ML threats. Other ML threats of concern, both foreign and domestic, include environmental crime, cybercrime (such as ransomware, hacking and website defacement), and drugs-related offences.

3.9 Singapore has not identified substantial ML/TF risks arising from these threats for now, but will continue to keep a close watch, to determine whether further mitigation measures and/or safeguards are necessary. Given increasing international attention to the ML risk arising from environmental crime (such as illegal wildlife trade and illegal logging) and to raise the industry’s awareness, a separate thematic risk assessment on ML related to environmental crimes was published on 29 May 2024⁴. The report noted Singapore’s inherent risks to ML related to environmental crimes arising from our geographic location and position as an international financial centre, trading, transport and transshipment hub.

Most commonly observed ML typologies - (i) Rapid pass-through of funds through bank accounts, (ii) misuse of legal persons such as shell companies, and (iii) placement in high value assets

3.10 Authorities in Singapore have observed a wide variety of laundering techniques being used in Singapore. Illicit funds flowing into or through Singapore are observed to be most commonly laundered via bank accounts, particularly as rapid pass-through transactions which involves cross-border transactions, and generally through the use of third-party

³ Singapore Financial System Stability Assessment; IMF Country Report No. 19/224; June 24, 2019

⁴ <https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/environmental-crimes-money-laundering-national-risk-assessment>

mules. Both corporate and individual mule bank accounts have been observed to be conduits exploited by money launderers, particularly where foreign criminal syndicates and professional money launderers are involved. In some cases where corporate mule accounts are involved, such individuals had also engaged CSPs to set up the companies.

- 3.11 **Consistent with international typologies, Singapore has noted that some legal persons (particularly, shell companies) are being misused⁵ for laundering of illicit funds through layering or concealment of ownership of illicitly obtained assets.** In particular, networks of Singapore-incorporated shell companies created and ultimately controlled by criminal networks have been used for ML purposes. The Companies Act requires each company to have at least one director who is ordinarily resident in Singapore⁶. Additionally, foreigners must engage the services of CSPs to incorporate a Singapore company. As such, a foreigner might also procure nominee director services from CSPs. While these requirements effectively subject foreign-owned/controlled Singapore companies and their nominee directors to AML/CFT scrutiny by the CSPs at the point of incorporation, there have been instances where CSPs were misused by foreign criminal elements to incorporate shell companies. After incorporation, the bank accounts of some such companies have been misused such that illicit proceeds could be channelled into and through Singapore under the guise of legitimate business transactions. Illicit proceeds are often used to purchase high value assets including real estate, precious stones, and precious metals.
- 3.12 **Considering the ML threats and vulnerabilities, the banking sector has been assessed to pose the highest ML risk to Singapore.** The role of banks in facilitating transactions in the financial system, and their wide networks through which cross-border transactions can be conducted, make banks a common channel which criminal exploit. In addition, banks are exposed to a larger proportion of customers with higher ML risks (including those from higher ML risk jurisdictions), high volume of cross-border transactions, and a range of complex products and structures.
- 3.13 Amongst the DNFBP sectors, CSPs are assessed to pose higher risks given the role they play in providing upstream services such as incorporation of companies. They have also been linked to the misuse of legal persons in some instances.
- 3.14 The other sectors which are assessed to be of higher risk and susceptible to ML include those which: (i) **facilitate cross-border transactions** (such as payment institutions with cross-border money transfer services, digital payment token services providers (DPTSPs)); (ii) act as **professional intermediaries which facilitate fund management through the use or management of complex ownership structures** (such as external asset managers, licensed trust companies); and/or (iii) **facilitate the integration of funds or placement of funds** in high value assets (such as real estate sector, casinos, precious stones and precious metals dealers). More detailed risk assessments (including the extent of each sector's exposure to ML threats, vulnerabilities, and strength of controls) can be found within the specific sectoral assessments.
- 3.15 International typologies⁷ have also noted that storage facilities, especially those in Special Economic Zones (SEZs), have been used to store high-value cultural objects, and such storage facilities may present ML/TF vulnerabilities. Singapore does not have any SEZ, and the Free

⁵ Singapore is separately conducting in-depth assessments of ML/TF risks arising from misuse of legal persons and legal arrangements.

⁶ Section 145(1) of Singapore's Companies Act.

⁷ FATF report on Money Laundering and Terrorist Financing in the Art and Antiquities Market

Trade Zones (FTZs) in Singapore do not have special storage facilities for high-value goods, including high-value cultural objects. The FTZs are used to facilitate entrepot trade through reduced formalities for the transshipment of goods and are largely used for intermittent storage of sea containers and other goods pending transshipment. There are also no banking, financial or auction entities operating in the FTZs. However, we are aware that the large volume of goods passing through the FTZs could increase Singapore's vulnerability to TBML and related risks. To address such concerns, Singapore's FTZ regime is designed to ensure strong governance of the FTZs to combat any criminal misuse (please see Annex on Singapore's Free Trade Zone Regime for further information).

4. INTRODUCTION TO SINGAPORE

4.1 GEOGRAPHY

- 4.1.1 Located in Southeast Asia, Singapore is an island city state with a land area of 725 square kilometres. Singapore has a population of around 5.92 million, of which 70% are residents.
- 4.1.2 Singapore's strategic geographical location has enabled it to develop into an international aviation and maritime transportation hub. Situated along the vital shipping lanes of the Straits of Malacca, Singapore is one of the busiest ports in the world, connected to more than 600 ports in over 120 countries and with more than 140,000 vessel calls annually. With an airport serving over 100 airlines flying to over 300 cities in about 80 countries and territories worldwide, Singapore has strong global connectivity.

4.2 ECONOMY

- 4.2.1 In 2023, Singapore's Gross Domestic Product (GDP) at current market prices was S\$673.3billion, with per capita GDP of S\$113,779. Singapore's top trading partners are China, Malaysia, the US and the European Union.
- 4.2.2 Singapore is a dynamic international business, financial and trading centre, characterised by economic openness, an efficient financial system and well-developed business infrastructure. Its diversified economy spans manufacturing, wholesale trade, finance/insurance and other services.
- 4.2.3 Singapore has been ranked by the International Monetary Fund (IMF) as one of 29 systematically important financial centres in the world and is host to more than 1,000 FIs offering a wide variety of financial products and services and serving a broad and diverse customer base. Singapore's financial centre is dominated by banks and features a highly efficient and developed system. Singapore is also one of the world's fastest growing wealth management centres, due primarily to the wide range of financial and wealth management services offered. As at end 2022, 76% of Singapore's assets under management originated from outside Singapore.⁸

4.3 SINGAPORE'S AML POLICY OBJECTIVES

- 4.3.1 Singapore's role as a regional and international business, financial and trading centre makes us vulnerable to being misused as a conduit for laundering of and destination point for illicit

⁸ 2022 Singapore Asset Management Survey, MAS.

funds. Ensuring that Singapore is protected against abuse by nefarious players is essential for our continued prosperity, since our development has been built on the hallmarks of strong rule of law, transparency and trustworthiness. Combating ML is therefore of national priority.

- 4.3.2 Overall, Singapore adopts a whole-of-system approach to preventing, detecting, and enforcing against ML, involving close coordination and collaboration amongst Government agencies, public-private partnership, and international cooperation.
- 4.3.3 Singapore's AML efforts are led by the AML/CFT SC, which comprises the Permanent Secretary of MHA, Permanent Secretary of the Ministry of Finance, and the Managing Director of MAS. The senior level involvement and the significant resources invested into AML work in Singapore demonstrate Singapore's strong commitment towards combatting ML.
- 4.3.4 The AML/CFT SC sets Singapore's policy objectives and directions for combating ML and ensures that the various government agencies have effective mechanisms in place to cooperate and coordinate with one another, and to strengthen Singapore's resilience against criminal abuse.
- 4.3.5 The AML/CFT SC is supported by the AML/CFT Inter-Agency Committee (IAC). The IAC which comprises Singapore's key AML agencies (including policy makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors, customs and tax authorities, intelligence services, the judiciary, etc), is the main operational body that facilitates the coordination and implementation of Singapore's AML policy. The SC and IAC are further supported by the RTIG, which is the main working level body tasked to review ML risks at the government level. The RTIG comprises all operational, law enforcement, regulatory, supervisory and policy agencies involved in AML/CFT work in Singapore. Through the IAC and RTIG, agencies also share information such as emerging ML threats and trends, FATF typologies, best practices and other developments.

4.4 ENFORCEMENT AND LEGAL FRAMEWORK

- 4.4.1 Singapore has a strong and transparent legal and institutional framework for ML enforcement, prosecution, asset recovery and international cooperation. Singapore continually keeps abreast of emerging AML developments and ensures that its legal and institutional framework are in line with international standards and best practices through providing leadership and actively participating at international and regional fora including the Financial Action Task Force (FATF), the Asia-Pacific Group (APG)⁹, the Financial Stability Board and Basel Committee on Banking Supervision, INTERPOL, and the Egmont Group.

Legislation and enforcement

- 4.4.2 Singapore's approach is to rigorously investigate all leads to uncover possible ML offences and we will not hesitate to prosecute offenders. In line with Singapore's key ML threats, agencies prioritise the investigation of complex, transnational ML cases perpetrated by

⁹ Singapore has served in various leadership roles at the FATF, including co-Chair of the FATF's Policy and Development Group, FATF Steering Group, and most recently FATF President (from June 2022 to June 2024). Through such active involvement, Singapore collaborates closely with fellow AML/CFT policy makers and experts to drive and develop international AML/CFT agenda and standards.

professional and syndicated money launderers. LEAs have the powers to access all necessary documents and information for use in investigations, prosecutions, and related actions. These include powers to compel production of records, search of persons and premises, taking of statements, and the seizure and confiscation of evidence and illicit assets. To ensure effective enforcement of ML cases, Singapore has a comprehensive framework for seizing and confiscating criminal proceeds (described below in paragraph 4.4.9).

- 4.4.3 Singapore has three key LEAs investigating money laundering – the (i) Singapore Police Force, which includes the Commercial Affairs Department (CAD), and Criminal Investigation Department (CID), (ii) Corrupt Practices Investigation Bureau (CPIB), and (iii) Central Narcotics Bureau (CNB). There are also other LEAs in Singapore who are responsible for investigating the predicate crimes, such as Inland Revenue Authority of Singapore (IRAS), Singapore Customs (Customs), National Parks Board (NParks).
- 4.4.4 The Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) is the primary legislation in Singapore which criminalises the laundering of criminal benefits and provides for the investigation and confiscation of such benefits. The penalty for an offence of ML is severe - imprisonment of up to ten years and/or fine of up to S\$500,000 for natural persons; and a fine not exceeding S\$1 million or twice the value of benefits of drug dealing or criminal conduct in respect of which the offence was committed, whichever is higher, for ML offences committed by legal persons.
- 4.4.5 Over the years, Singapore has further strengthened our AML levers, to ensure that our laws remain effective and relevant¹⁰:

CDSA

- On 1 April 2019, the CDSA was enhanced to (i) introduce a new ML offence to criminalise the possession or use of property reasonably suspected of being criminal proceeds, if the accused cannot satisfactorily account for it; (ii) allow the Courts to decide on ML cases involving overseas crimes on the basis of evidence presented by the Prosecution, without having to rely on foreign governments or experts; (iii) allow for higher maximum fines for ML offences committed by legal persons; and (iv) allow STRO to exchange information under an international arrangement, subject to there being an undertaking to ensure reciprocity as well as safeguards to protect the confidentiality of information shared and control their specific use¹¹.
- In May 2023, the CDSA was enhanced to introduce new money laundering offences that would enable LEAs to prosecute persons for a money laundering offence at lower levels of culpability. Amongst the enhancements, it is an offence for a person if he engages in any of the specified conduct as prescribed in the laws, regardless of his level of knowledge of the offence. The introduction of tougher laws is part of Singapore's efforts to mitigate the abuse of Singapore's financial system for laundering of illicit funds, especially in relation to scams.

¹⁰ Authorities will be amending relevant laws to enhance the ability of our law enforcement agencies to pursue and prosecute offenders for money laundering. These laws are expected to be passed in Parliament in the second half of 2024.

¹¹ This has allowed STRO to exchange financial intelligence with more than 150 overseas counterpart financial intelligence units which are members of the Egmont.

Other Laws

- In February 2018, legislative amendments were made to the Computer Misuse Act (CMA) to pave the way for the operationalisation of the Cybersecurity Act 2018 and enhance LEAs' ability to pursue cybercrime more effectively. This serves to tackle the increasing scale and transnational nature of cyber threats and the evolving tactics of cyber criminals and empower investigators where computer-related evidence is involved. In the same year, the Criminal Reform Justice Act 2018 and the Evidence (Amendment) Act 2018 were passed in the Parliament and empowers relevant investigators to access, secure and safeguard evidence on computers, regardless of whether the evidence is stored on a computer inside or outside Singapore.
- The CMA was amended in May 2023 to criminalise the disclosure and obtaining or dealing in Singpass¹² credentials to facilitate criminal activities. These amendments seek to curb the abuse of Singpass by deterring individuals from enabling or facilitating the commission of criminal activities such as fraud and money laundering by others and to protect citizens and businesses who depend on Singpass as our national digital identity.
- On 1 February 2024, the Online Criminal Harms Act (OCHA) came into effect, and it introduced levers to enable authorities to more effectively deal with online activities that are criminal in nature. Such offences include ML and specified predicate offences. With OCHA, the Government may now issue directions against specified criminal offences, proactively prevent cyber-enabled fraud and malicious cyber activities through requiring designated online services to comply with Codes of Practice and Directives.
- In 2018, the Goods and Services Tax Act (GSTA) and Income Tax Act (ITA) were amended to enhance investigation powers for IRAS officers, such as the powers of arrest and forced entry when investigating tax crimes. In 2020, these powers were further enhanced under the GST Amendment Act 2020, allowing officers to seize goods suspected to be used to commit an offence under the GSTA (instrumentalities of crime). Such powers enhance IRAS' ability to combat and disrupt the commission of tax offences.
- In October 2023, the Free Trade Zones Act (FTZA) was amended to enhance the regulation and control of goods that flow through our FTZs. Amendments include the introduction of a licensing regime for FTZ operators, and prescribing data provision requirements for FTZ operators and cargo handlers on goods flowing through the FTZs. These amendments enhance Singapore Customs' (Customs) oversight of the entities operating within the FTZs and ability to detect illicit activities taking place in the FTZs.

4.4.6 STRO maintains close working relationships with various law enforcement, intelligence, and supervisory agencies, both domestically and internationally, and regularly disseminates financial intelligence to them. Financial intelligence has also proven to be very useful in identifying leads otherwise unknown to LEAs and providing leads to ongoing investigations.

¹² Singpass stands for Singapore Personal Access, which is Singapore's national digital identity. Users can use Singpass to transact with Government agencies and private sector organisations. Currently, Singpass has more than 4.5 million users, covering 97% of Singapore Citizens and Permanent Residents aged 15 and above.
Source: www.smartnation.gov.sg.

- 4.4.7 Singapore, represented by CPIB, is a founding member of the IACCC, which coordinates global law enforcement responses to allegations of grand corruption.¹³ Law enforcement agencies on board the IACCC can carry out simultaneous checks and information exchanges with agencies from various jurisdictions that are also major financial centres, thus allowing for timelier restrains of illicit proceeds¹⁴.

Central BO Registry

- 4.4.8 In addition, Singapore has enhanced LEAs' and AML/CFT supervisors' access to beneficial ownership information on legal persons. In March 2017, Singapore amended our laws to require companies and limited liability partnerships (LLPs) to obtain and maintain BO information, to ensure that accurate BO information is readily available to competent authorities. Further, Singapore set up a central non-public BO register, a significant step towards enhancing BO transparency. From 30 July 2020, all companies and LLPs are required to submit their BO information to ACRA. Information within the central BO register, maintained by ACRA, is directly and immediately accessible to competent authorities for the enforcement of any written law in Singapore. ACRA continues to strengthen the effectiveness of the central BO register, including taking measures to ensure greater accuracy of the BO information maintained. ACRA is also studying how access to ACRA's central BO register can be expanded to more parties and is establishing strong relationships with international counterparts to learn from their best practices.

Asset Recovery

- 4.4.9 **Asset recovery is a fundamental tenet in Singapore's fight against ML and other crimes.** We need to send a strong, deterrent message that Singapore is determined to deprive criminals of their illicit gains. This removes the key motivation for financial crime, while providing reprieve for the victims. Maximising the recovery of criminal assets is a key aspect of the operating paradigm of law enforcement agencies. Singapore's **National Asset Recovery Strategy**, which will be detailed in a paper to be released in 2H 2024, comprises four pillars:
- (i) **Detect** suspicious and criminal activities, including the proceeds of crime and instrumentalities of crime;
 - (ii) **Deprive** criminals of their ill-gotten proceeds through prompt seizure and confiscation;
 - (iii) **Deliver** maximum recovery of assets for forfeiture and restitution to victims; and
 - (iv) **Deter** criminals from using Singapore to hide, move, or enjoy their illicit assets.

¹³ The IACCC is based in London and hosted by the UK National Crime Agency (NCA). Besides CPIB Singapore and the UK NCA, IACCC members include the Australian Federal Police, the Netherlands Fiscal Information and Investigation Service, New Zealand's Serious Fraud Office, New Zealand Police, Royal Canadian Mounted Police, US' Federal Bureau of Investigation, US Department of Homeland Security, Immigration and Customs Enforcement and Homeland Security Investigations.

¹⁴ For example, IACCC received a referral in April 2021 alleging that Country A's PEP was involved in grand corruption. IACCC associate members were roped in at an early stage to identify links and trace assets in offshore jurisdictions. As a result, by March 2022, a total of EU€120 million (approximately S\$175.8 million) worth of assets were frozen, with IACCC assisting to freeze assets in the UK worth tens of millions of pounds.

Prosecution & the Court System

- 4.4.10 AGC is an independent Organ of State, and 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 MLA and extradition. It also provides legal advice to government departments and LEAs on the interpretation of AML/CFT laws and issues.
- 4.4.11 Based on investigations by LEAs, the Public Prosecutor controls and directs all criminal prosecutions and proceedings in Singapore. This includes applying to the Courts for a confiscation order against a defendant in respect of the benefits derived from criminal conduct.
- 4.4.12 The Courts play 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.

4.5 INTERNATIONAL COOPERATION

- 4.5.1 The transnational nature of crimes has heightened the need for Singapore authorities to engage in international cooperation in our fight against crime.

Formal Cooperation

- 4.5.2 Singapore is able to provide a wide range of assistance to other jurisdictions without the need for a bilateral MLA treaty on the basis of reciprocity under the Mutual Assistance in Criminal Matters Act (MACMA). AGC has clear and efficient processes in place to deal with formal requests in a timely manner. Generally, AGC would be able to process and execute incoming MLA requests within the established timelines if the MLA requests meet the requirements under the MACMA.
- 4.5.3 In line with FATF Recommendation 37, the MACMA allows Singapore to provide a wide range of MLA, such as production, search and seizure of information, documents or evidence, as well as asset recovery. MLA is generally available notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Where dual criminality is required, it is satisfied if both the requesting country and Singapore criminalise the conduct underlying the offence, regardless of how each country labels the offence.
- 4.5.4 Singapore also has an effective extradition regime, with a wide network of extradition partners, including declared Commonwealth jurisdictions and bilateral as well as multilateral treaty partners. In 2022, Singapore introduced several amendments to update and modernise our extradition regime. A key amendment was the adoption of a threshold approach for determining whether an offence is extraditable, i.e. our Extradition Act now provides that an offence is extraditable as long as it has a maximum punishment of two years' imprisonment or more and is not on a list of excluded offences. This replaced the positive list approach, where only offences described in a list would be extraditable. In recent years, Singapore has successfully extradited individuals for ML-related offences.

Informal Cooperation

- 4.5.5 Apart from using formal international cooperation channels such as MLA and extradition, authorities continue to seek opportunities for other forms of (informal) cooperation. This includes cross-border joint investigations and membership in relevant operational platforms to encourage exchange of information via LEAs, FIUs, and tax agencies. Supervisory authorities also have arrangements in place to allow for cooperation and/or the exchange information with their foreign counterparts including for pertinent concerns such as ML/TF risk management and controls, to facilitate effective supervision of their entities.
- 4.5.6 The Police have formed cross-border joint investigation teams with foreign counterparts, in jurisdictions such as Malaysia, Hong Kong, Macau and China, to disrupt transnational criminal syndicates. Between 2021 and 2023, 48 syndicates and 345 persons were arrested overseas in relation to cyber-enabled fraud targeting Singapore residents and laundering their ill-gotten gains out of Singapore. Further, to tackle the transnational risk posed by unlicensed money lending (UML) syndicates, the Police collaborate closely with foreign counterparts through intelligence exchanges and bilateral exchanges. These efforts have resulted in several cross-border joint investigations over the years.
- 4.5.7 Apart from joint investigation teams, LEAs also leverage INTERPOL's network to connect with other law enforcement units globally. Singapore has supported various initiatives organised by INTERPOL, including operational efforts such as Operation First Light and Operation Haechi, both of which involved global crackdowns on impersonation scams and cyber-enabled crime. In particular, CAD has benefited from a secondment to the INTERPOL Financial Crimes Unit. Singapore joined ARIN-AP in 2017 and is one of the 9 Steering Group members since 2024. ARIN-AP aims to bring about improvements to the speed and reactivity of countries' asset recovery efforts on an informal basis, prior to countries utilizing MLAs.
- 4.5.8 Singapore has been an Egmont member since 2000. Since 1 April 2019, legislative amendments were introduced to the CDSA to allow STRO to exchange information with members of the Egmont Group, an international body of Financial Intelligence Units recognised by the FATF and organised to enhance international cooperation. With the expansion in the network for information exchange, STRO saw a 23% increase in the number of incoming requests for assistance requests from our foreign counterparts in 2019 as compared to 2018. In addition, STRO participates in various international and regional projects, such as those under the Egmont Group as well as the Financial Intelligence Consultative Group co-chaired by the FIUs of Australia and Philippines.
- 4.5.9 The London-based IACCC seeks to enhance information sharing by bringing together specialist law enforcement officers from multiple jurisdictions into a single location. Since its establishment in July 2017, the IACCC has sped up global grand corruption investigations through both information sharing and the provision of technical/operational support, which in turn led to the restraint of a significant amount of assets¹⁵. Being on board the IACCC since

¹⁵ On a case involving a former PEP who allegedly embezzled state funds from a Middle Eastern country, the IACCC assisted to identify approximately GB£8 million worth of properties linked to the suspects to support the home country's investigation. The IACCC is also rendering assistance to Country X on multiple grand corruption investigations, for which over US\$1 billion of assets has been frozen for one of the cases. In another high-profile case, IACCC identified GB£9 million worth of jewellery in a foreign jurisdiction and assisted to have the assets frozen temporarily for the home country carrying out the investigations to secure an order to seize the assets.

its inception has allowed Singapore to be in the loop of high-profile grand corruption cases at a relatively early stage. More recently, CPIB facilitated a meeting between the Central Authorities of two jurisdictions to discuss asset recovery matters and received positive feedback for our efforts.

- 4.5.10 In keeping with our commitment to international standards on transparency and tax cooperation, Singapore has implemented the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS) in 2014 and 2017, with first exchanges under FATCA and CRS in 2015 and 2018 respectively¹⁶. Since its first exchanges, IRAS has transmitted CRS and FATCA information to all reciprocal partner jurisdictions and the US respectively within the exchange deadline and continues to do so with all interested and appropriate partners annually.

Case Study 1 – Singapore’s assistance in securing the conviction and penalties against Bernie Ecclestone

Singapore was a crucial partner in the conviction of Bernie Ecclestone on 12 October 2023, and the recovery of assets involved in the criminal activity.

The United Kingdom tax authority, His Majesty’s Revenue and Customs (HMRC), had launched a lengthy, complex and worldwide investigation into his tax affairs since more than a decade ago, against Formula One motor racing boss, Bernie Ecclestone. He failed to declare a trust which held assets of more than GB£416 million.

Bernie Ecclestone had claimed that he was not the settlor or beneficiary of any offshore trust based on interviews with UK tax investigators in 2015. However, information was proactively shared by Singapore authorities with UK authorities through the FIU and LEA channels to provide crucial support to the UK’s investigations and showed that claims were untrue. The close cooperation between CAD, STRO and the relevant UK authorities is testament to Singapore’s commitment to international cooperation, to achieve effective outcomes in the common fight against transnational crime.

Bernie Ecclestone was eventually sentenced to 17 months in prison, suspended¹⁷ for two years in London, and has made a payment of more than GB£650 million in relation to his tax affairs, covering tax penalties and civil penalties.

¹⁶ The FATCA was enacted by the US Congress to target non-compliance with US tax laws by US persons using foreign accounts while the CRS is an internationally agreed standard for the automatic exchange of financial account information between jurisdictions for tax purposes, to better combat tax evasion and ensure tax compliance. An entity that falls within the definition of a Reporting Singaporean Financial Institution (RSGFIs) under the CRS and/or FATCA regulations is required to register under the respective standard, and identify and report the Beneficial Owners/Controlling Persons of financial accounts maintained in Singapore by Passive Non-Financial Entities, or in the case of a trust managed by trustees, its settlor(s), beneficiary(ies) and protector(s) where they are residents of Reportable Jurisdictions under the CRS, or are US Persons under FATCA.

¹⁷ Under the UK’s sentencing regime, suspended sentences are custodial sentences where the offender does not have to go to prison provided, they commit no further offences and comply with any requirements imposed.

4.6 SINGAPORE'S APPROACH ON ML RISK SURVEILLANCE AND ASSESSMENT

- 4.6.1 The RTIG regularly discusses Singapore's key ML threats and risk considerations, including cases, typologies and vulnerabilities identified and recommends mitigation steps.
- 4.6.2 To further support efforts on this front, the RTIG has in place an inter-agency case prioritisation framework to facilitate the detection, prioritisation, and coordination of significant ML cases across agencies. To strengthen detection capabilities, an inter-agency taskforce, the Inter-Agency Suspicious Transaction Report Analytics Taskforce (ISTRA), was formed in 2018 under the auspices of RTIG. ISTRA, comprising representatives from MAS, STRO and LEAs, identifies, prioritises and reviews suspicious transaction reports (STR) for the identification of significant ML activity in Singapore, for possible regulatory and/or enforcement actions. By overlaying financial intelligence with information from other sources such as business registration information, transactional data, intelligence leads from LEAs, ISTRA leverages its data analytics capabilities to identify hotspots of suspicious activity. This has allowed relevant law enforcement and supervisory authorities to (i) enhance processes allowing for better identification of complex and sophisticated forms of ML for more focused detection of suspicious networks; and (ii) pursue foreign predicate ML, such as those relating to professional and syndicated ML, TBML and the misuse of shell companies, in line with Singapore's inherent risk profile.
- 4.6.3 As part of the RTIG process, regulatory and supervisory agencies also conduct ongoing risk surveillance and share information involving any key and emerging risk concerns identified within their sectors for mitigation action. They also perform regular outreach activities to enhance ML risk awareness within their sector. STRO supports this work through the development of strategic analysis products derived from STRs and other intelligence, which they disseminate to relevant law enforcement and supervisory authorities. Where appropriate, STRO has also worked with relevant LEAs and supervisors to further develop and share suitable risk products with the industry.
- 4.6.4 RTIG's and Singapore's risk surveillance is enriched by insights gathered from industry, which includes emerging trends and typologies observed from their lenses. This could be through industry partnerships, industry associations or direct feedback between entities and their supervisors. Examples of industry partnerships include the AML/CFT Industry Partnership (ACIP), Alliance of Public Private Cybercrime Stakeholders (APPACT) and Anti-Corruption Partnership Network (ACPN)

AML/CFT Industry Partnership (ACIP)

- 4.6.5 ACIP was set up in April 2017 to bring together stakeholders from industry and government and provides a dedicated platform for the discussion of key transnational illicit financial risks confronting Singapore's financial and DNFBP sectors. It also supports the identification and promotion of focal areas to uplift the implementation of AML/CFT measures in Singapore.
- 4.6.6 ACIP helps to drive risk understanding, assessment and mitigation across the system. For example, ACIP has established a Risk and Surveillance Workgroup to proactively monitor and strengthen surveillance and understanding of emerging risks. It has also set up relevant working groups to look into key industry risk concerns such as (i) the misuse of legal persons and arrangements, (ii) digital assets risk management, and (iii) proliferation financing.

- 4.6.7 ACIP has developed risk mitigation products to strengthen the broader industry's understanding and mitigation of such key risks. For example, in May 2018, ACIP published two industry best practice papers relating to the typologies of abuse of legal persons and trade-based money laundering/trade financing, including preventive measures. More recently, ACIP published a number of best practice papers aimed at addressing key risks concerns, including managing risks from customer relationships with nexus to digital assets, and risks associated with dealing with customer referrals from corporate services providers. These ACIP products feed into this NRA process. MAS and CAD also work together with banks through ACIP to disseminate alerts on emerging risk typologies observed from cases and other sources of information to raise awareness within the industry.
- 4.6.8 LEAs share tactical information on specific cases with relevant financial institutions, under the case-specific information sharing (CSI) mechanism within ACIP. This facilitates joint investigations and collaboration amongst LEAs, STRO and the banks and has achieved successful results. For instance, it was through the CSI mechanism that one of the largest cases of trade financing fraud in Singapore involving Agritrade International Pte Ltd (Agritrade) was detected. In January 2023, the former Chief Financial Officer of Agritrade was convicted and sentenced to 20 years of imprisonment for offences relating to cheating and falsification of accounts.

Alliance of Public Private Cybercrime Stakeholders (APPACT)

- 4.6.9 Cybercrime is an emerging area of concern. The SPF Cybercrime Command established APPACT as a public-private partnership in 2017 to exchange information among partners on suspicious cybercrime activities and latest trends and increase operational effectiveness.
- 4.6.10 APPACT comprises partners from various industries such as financial institutions, telecommunications service providers and cryptocurrency businesses. APPACT partners have been providing strong support to cases investigated by SPF, as seen during the cyber-enabled fraud reports involving OCBC accounts in end 2021 and more recently in cases involving malware cyber-enabled fraud. Apart from that, APPACT partners have provided investigative leads to SPF and shared their threat analysis report for both the local and overseas region. At the regional level, various APPACT partners are invited to conduct their sharing at events such as the ASEAN Plus Three Cybercrime Conference (APTCC), ASEAN Senior Officials Roundtable on Cybercrime (SORC) and ASEAN Senior Officials Meeting on Transnational Crime (SOMTC).

Anti-Corruption Partnership Network (ACPN)

- 4.6.11 The Corrupt Practices Investigation Bureau (CPIB) established the ACPN in 2018 with the objective of promoting ownership and collaboration on the prevention of corruption within the private sector. The ACPN started with 25 members and has since grown to 70 entities to include financial institutions, select auditing and consultancy firms, professional bodies, and industry associations. Since the inaugural engagement session in 2018, CPIB has held annual ACPN events with members, to inculcate a culture of anti-corruption and integrity in the private sector.

5. ML NRA METHODOLOGY

- 5.1 The methodology used for this NRA (see Table 1) is aligned with the FATF's Guidance and also takes reference from the World Bank's NRA methodology.¹⁸ It is a function of threats (taking their consequences and impact into account), vulnerabilities and controls, with greater emphasis accorded to threats and vulnerabilities. In determining the ML risk to Singapore, Singapore's economic and legal framework, and a broad range of qualitative and quantitative threats, vulnerabilities and control factors was considered.

Table 1: ML NRA Methodology

Threats*	<ul style="list-style-type: none">• ML/TF cases, prosecutions & convictions• MLA and other formal/informal requests for assistance/cooperation• STRs, intelligence• Regional/global typologies & relevant reports• Surveys of/discussion with foreign LEA/FIU partner
Vulnerabilities	<ul style="list-style-type: none">• Exposure to key threats• Higher risk customers/jurisdictions• Cross-border transactions• Complexity of structures/products• Cash intensity• Size and significance
Controls	<ul style="list-style-type: none">• Legal and supervisory framework• Industry's ability to drive sector-wide initiatives• ML/TF risk management framework• Risk awareness & understanding• Risk detection and mitigation techniques & STR reporting capabilities• Contribution to public-private partnership

**Taking their consequences¹⁹ and impact into account.*

Determination of ML Threats

- 5.2 The ML NRA methodology is anchored by Singapore's exposure to ML threats as a whole, and as applicable to each sector. Key ML threats for Singapore were determined through a detailed analysis of a broad range of indicators, which have been identified based on the five guiding principles:

- (i) **Understanding of Singapore's crime threat landscape**, by assessing the prevalence of predicate offences originating in Singapore and abroad. Indicators considered include convictions under predicate offences, quantum of proceeds of crime

¹⁸ Reference was taken from the Guidance on National Money Laundering and Terrorist Financing Risk Assessment published by the FATF in February 2013 and the Introduction to the National Risk Assessment Tool published by the World Bank in June 2015.

¹⁹ The impact or harm that ML may cause, including the effect of the underlying criminal activity on financial systems and institutions.

involved, STRs tagged to predicate offences, as well as formal and informal international cooperation requests.

- (ii) **Extent of ML activity that had materialised in Singapore**, by considering indicators such as ML investigations, prosecutions and convictions arising from the respective crime threat.
- (iii) **Singapore's inherent exposure to crime based on its environmental and contextual factors**. Insights and observations were drawn from international and regional reports. Key threats to Singapore arising from key typologies seen regionally and internationally were also factored in qualitatively. The assessment also examined if crime threats that have materialised regionally or globally would have manifested in Singapore given our inherent risk profile.
- (iv) **Propensity to launder proceeds in Singapore**. Authorities' insights, including from LEA experts, were used to assess the likelihood of particular predicate crimes crystallising into ML activities in Singapore. Indicators that would affect the propensity to launder proceeds in Singapore include the structure/complexity of the criminal element, profile of criminals and potential quantum involved.
- (v) **Singapore's ML threats from the lenses of its key foreign partners**. To enhance its risk understanding in respect of its foreign ML threats, this factor focuses on key ML threats to Singapore as seen from the lenses of its key foreign LEA and FIU partners. We have surveyed our key foreign law enforcement and financial intelligence partners. The survey results were enriched with targeted discussions with relevant partners. This allowed Singapore to better evaluate our foreign ML threats.

Sectoral risk - Vulnerabilities and controls

- 5.3 The establishment of Singapore's key ML threats brings us to the next step of the methodology, which is to consider the vulnerability²⁰ of every relevant sector in Singapore, based on its exposure to the key ML threats identified and the likelihood of such threats materialising within the sector. As the threats posed to and vulnerabilities faced by each sector are mitigated to some extent by the strength of the sector's AML/CFT controls²¹, these relevant factors were also considered, in order to derive the overall ML risk posed to Singapore by the sector. For the purposes of this NRA, all relevant sectors in Singapore were considered against the factors laid out in Table 2. Hence, each sector's ML risk level contained a consideration of (i) the inherent ML threat to the sector; (ii) the sector's vulnerability to ML; and (iii) the prevailing level of AML/CFT controls the sector has in place.

²⁰ Vulnerabilities are things that can be exploited by threat or that may support or facilitate its activities.

²¹ Measures that can help to combat ML or mitigate vulnerabilities to ML.

Table 2: Factors considered to determine sectoral ML risk

Risk/Control Factors	
Threat	Level of exposure to key ML threats
Vulnerability	Proportion of customers that pose higher ML risk
	Proportion of customers from higher ML risk jurisdictions
	Proportion of cross-border transactions
	Use of complex products/structures
	Physical cash intensity
	Size and significance
Controls	Maturity of legal and supervisory framework
	Ability of industry association(s) to drive sector-wide AML initiatives
	Strength of ML risk management framework and processes (includes level of risk governance and oversight, and robustness in execution of controls)
	Level of ML risk awareness and understanding
	Use of advanced risk detection and mitigation techniques, and maturity of suspicious transaction reporting capabilities
	Contribution to public-private collaboration

- 5.4 It should also be noted that ML risk ratings are based on an assessment of relativity, and a lower risk rating does not mean that there is no risk within the sector. ML may continue to occur within lower ML risk sectors and all sectors or areas covered in this NRA are assessed to be exposed to some level of ML risk.

6. MONEY LAUNDERING THREAT

6.1 OVERVIEW OF KEY NATIONAL ML THREATS

- 6.1.1 Singapore consistently has a low domestic crime rate, due to our strong and transparent rule of law as well as effective enforcement and prosecution. That said, we note a marked increase in threat posed by domestic fraud, specifically cyber-enabled fraud. In addition, as an international business, financial and trading centre with a significant non-resident population, Singapore is exposed to external threats arising from foreign predicate offences which result in their proceeds flowing into or through our system. This assessment is supported by the take-aways from our engagements with foreign counterparts – that Singapore faces higher ML risks arising from foreign threats, as opposed to domestic threats. Overall, the openness of Singapore's economy and the high level of connectivity to other financial and trading centres expose our system to the risk of being misused for ML, TF, PF and other financial crimes.
- 6.1.2 Given the application of the ML NRA methodology, a number of key ML threats has been identified for Singapore. The following sections cover the foreign ML threats, and the domestic ML threats which Singapore faces.

6.2 FOREIGN ML THREATS

- 6.2.1 Singapore's major ML threats derived from predicate offences committed abroad are fraud, organised crime, ML, corruption, tax crimes, and TBML.

Fraud, particularly Cyber-enabled Fraud

- 6.2.2 Singapore's highest foreign ML threat emanates from fraud. This is in line with the trend seen regionally and internationally, where fraud has been frequently highlighted as a key ML threat for a large number of jurisdictions²². As a regional and international business, financial and trading centre, Singapore is vulnerable to being misused as a conduit to launder illicit funds derived from fraud committed abroad. Fraud is also the top predicate crime mentioned by other jurisdictions to pose a ML threat to Singapore. Referencing INTERPOL reports, financial fraud is a predatory crime which is perpetrated in anonymity and across borders. In particular, financial fraud is a fast-evolving threat in the region.
- 6.2.3 Fraud is the most commonly cited offence raised by foreign authorities in their requests to Singapore for assistance, whether through the FIU or LEA route. These incoming requests resulted in a higher number of ML investigations, and consequently prosecutions and convictions in Singapore. LEAs have also found that fraud is the most common foreign predicate offence investigated in our ML cases. A frequently observed modus operandi includes foreign victims of BEC cases being deceived into sending their funds to Singapore.
- 6.2.4 The ML threat from fraud was amplified during the Covid-19 pandemic. The FATF report on Covid-19 related ML/TF risks found that criminals had attempted to profit from the pandemic through increased fraudulent activities, such as the impersonation of officials, counterfeiting of essential goods, fundraising for fraudulent charities and fraudulent investment scams.
- 6.2.5 Fraudulent funds derived from abroad are often laundered in Singapore via third parties, instead of being self-laundered. LEAs have observed patterns of increased syndication and sophistication, at times involving multiple layers of corporate and individual mules. The following case study shows a syndicated network of money mules recruited in Singapore to launder foreign fraudulent proceeds.

Case Study 2 – Syndicated network of money mules

Two Singapore nationals conceived and operated a multi-tiered professional ML network that involved recruiting friends and family members as money mules. They had been introduced to a business opportunity by friends based in Country A to contacts in Country A, and subsequently agreed to assist these contacts to launder criminal proceeds.

In addition to receiving criminal proceeds in their bank accounts, the duo recruited seven other individual mules to similarly use their corporate and individual bank accounts to launder cyber-enabled fraud proceeds for criminals in Country A. Between December 2013 and June 2017, a total of 25 corporate and individual bank accounts were used to receive approximately S\$1.35 million of criminal proceeds. These monies were then withdrawn in cash and physically transported to criminals in Country A on 32 occasions, without the requisite cross-border cash declarations being made.

²² Based on MERs review of 29 FATF and 30 FSRB members [FATF AGSR document]

As of May 2024, one of the two masterminds was convicted of money laundering and sentenced to imprisonment of 84 months and four weeks while court proceedings against the other are still ongoing. Six of the seven individuals have been warned or sentenced to a range of three to 24 months' imprisonment, for varying involvement in facilitating the professional money laundering scheme. Investigations and/or prosecutions are still in progress against the remainder of the seven mules.

- 6.2.6 Where corporate mules are concerned, our investigations as well as typologies research suggests that foreign criminal elements have tried to obscure their identities by recruiting nominee directors to meet local regulatory requirements when incorporating shell companies²³. Such shell companies were observed to be used to conduct illicit funds transfers. Some of these shell companies were formerly "shelf companies"²⁴ that had been sold to customers by CSPs. These observations are commensurate with STRO's review of STRs filed by CSPs, where fraud and ML were the top suspected crime types reported by the sector.
- 6.2.7 The misuse of legal persons is also often associated with the misuse of corporate bank accounts. Investigations have shown that corporate bank accounts in Singapore have been used to layer illicit funds, particularly for pass-through transactions. These legal persons appeared to be using Singapore as transit point to receive and transfer illicit proceeds from and to other jurisdictions. The following case study shows the swift actions taken by LEAs in Singapore against a professional money launderer who had laundered proceeds through his corporate bank account into Singapore, arising from a foreign BEC scam.

Case Study 3 – Illicit funds from foreign BEC victim seized in Singapore

In the wake of medical supply shortages caused by the Covid-19 pandemic, a French pharmaceutical company was defrauded into transferring monies from France to a Singapore company as payment for surgical masks and hand sanitisers. The French pharmaceutical company had made payment for supplies amounting to EU€6.64 million from their usual supplier, whose identity had been stolen through a BEC scam.

When the Singapore bank received a funds recall message from the French pharmaceutical company, it quickly raised an alert to CAD. Given the international component of the transaction, CAD immediately notified their French counterparts of the suspicious money inflow and the possibility of fraud. Through swift intervention and collaboration with the banks, the ASC of the CAD seized over EU€4 million on the day the alert was raised.

An individual, who is the director of the Singapore incorporated company, was charged on suspicion of laundering scam proceeds. The director has since been charged for ML offences and other offences. As of May 2024, court proceedings are ongoing.

²³ Singapore requires all companies are required to have at least one director resident in Singapore, to ensure that a resident individual can be held accountable for any breaches committed by the company in Singapore. This goes beyond the FATF's recommendations, and few comparable jurisdictions have this additional requirement.

²⁴ Shelf company refers to an incorporated company with inactive shareholders, directors and secretary, which has been left dormant.

- 6.2.8 To a lesser extent, LEAs have further observed ML typologies arising from foreign fraud cases involving the DNFBP sector. For example, illicit proceeds from a Ezubao Ponzi scheme in China involving 1.15 million Chinese victims were found to be routed to Singapore via bank transfers for the purchase of private real estate in Singapore. The real estate purchase was facilitated by a lawyer and a real estate agent, both of whom have been found to have failed to comply with their STR filing obligations. They have been convicted in 2018 for the breach and fined S\$10,000 each (see Case Study 43).

Organised Crimes (Illegal online gambling)

- 6.2.9 Compared to terrestrial gambling, remote gambling gives greater cause for concern. First, it carries a higher degree of lucrativeness and higher tendency to be transnational in nature. Remote gambling operations are lucrative and can potentially become a source or conduit of funds for ML and other illegal activities. These operations are transnational and of a significant scale, taking bets from a multitude of players across many countries. Second, remote gambling is ubiquitous and easily accessible, due to the reach of the internet, affordable mobile bandwidth, and proliferation of smart and mobile devices. Remote gambling was criminalised in Singapore in 2014, covering the spectrum from individual gamblers to facilitators, agents, and runners. To address the transnational nature of remote gambling activities, prohibition of remote gambling activities would apply to facilitators and remote gambling operations even if they reside overseas, as long as their customers are in Singapore.
- 6.2.10 Despite strict laws and regulations against online gambling, and multi-pronged enforcement actions, syndicates are still able to conduct illegal online gambling activities due to the ease of setting up or shutting down of an illegal online gambling site. The ability to host these illicit websites outside of Singapore makes clamping down on illegal gambling a challenge for LEAs. Syndicates are also able to use alternative payment methods such as cryptocurrencies and illegal payment platforms which make the detection of suspicious transactions or money tracing difficult.
- 6.2.11 A recent major money laundering case has demonstrated the impact of ML from foreign organised crime syndicates in Singapore. Ten foreign individuals were apprehended for money laundering activities, revealing an established foreign syndicate operating in Singapore's financial hub, and making it one of the biggest AML busts in Singapore's history. Investigations revealed that these syndicates were funnelling money from illegal online gambling and were associated with Chinese illegal gambling syndicates which operate internationally.

Case Study 4 – ML Threats and Risks in Singapore's Recent Major Money Laundering Case

On 15 August 2023, ten suspects were arrested in a series of simultaneous raids at multiple locations across Singapore. As part of the ongoing investigations, more than S\$3 billion²⁵ of suspected illicit financial and physical assets, including cash, cryptocurrencies and luxury goods were seized or prohibited from disposal, in one of Singapore's largest anti-money laundering operations.

This operation was achieved arising from the close cooperation and coordination of actions among law enforcement, intelligence (including STRO) and supervisors (such as MAS and ACRA).

²⁵ As at 31 January 2024

Case background:

- Elements of the case had earlier been identified from different information sources on suspicious activities including reports on the use of suspected forged documents to substantiate sources of funds in bank accounts, and STRs filed by FIs and other companies.
- In early 2022, Police launched a comprehensive, coordinated intelligence probe. The probe uncovered a web of individuals believed to have connections amongst themselves, including familial ties. By August 2023, Police had gathered sufficient evidence to take action.
- Ten persons were arrested and charged for offences including laundering proceeds from suspected overseas criminal activities, including online gambling, and more than S\$3 billion of assets in Singapore were seized or prohibited from disposal. As of June 2024, the assets which have been seized or prohibited from disposal include:
 - Approximately 222 properties.
 - Monies in bank accounts amounting to more than S\$1.5 billion, cash (including foreign currencies) amounting to more than S\$79 million, cryptocurrencies valued at more than S\$38 million (at time of seizure).
 - Numerous luxury and valuable assets such as precious stones and metals including jewellery and watches, as well as luxury bags.
- In addition to ML, some of the accused have been charged with forgery, making of false representations, resisting arrest and perverting the course of justice under the Penal Code 1871, and false declaration under the Employment of Foreign Manpower Act 1990.
- LEAs worked closely with STRO and supervisory agencies to identify networks, assets and further investigate this case.
- As of June 2024, ten suspects have been convicted of money laundering and other offences and sentenced to imprisonment of between 13 and 17 months. Eight of them have been deported after serving their sentence and barred from re-entering Singapore. At least 90% of the properties seized from the ten convicted persons, totalling more than S\$944 million, have been forfeited to the State.
- Investigations are ongoing against 17 persons who are not in Singapore.

Key ML threats and risks observed:

From investigations so far, the assets seized and prohibited from disposal are believed to be proceeds from criminal activities and predicate offences outside of Singapore. These activities were suspected to include **illegal online gambling**.

The proceeds were laundered through Singapore across the following key sectors:

- **FIs:**
 - FIs had detected suspicious activities and filed numerous STRs on the persons of interest. These STRs helped STRO and LEAs identify and take appropriate actions.
 - Around S\$1.5 billion in financial assets were seized from the accounts that the persons of interest continued to hold with FIs in Singapore.
- **Real estate sector:**
 - The persons of interest had purchased more than 200 properties in Singapore through real estate agents and developers. In some cases, they had purchased multiple properties in the same project, ostensibly for investment purposes.
 - In addition, 6 of the persons arrested were residing in properties under rental arrangements in Singapore.

- **Precious Stones & Precious Metals Dealers (PSMDs):**

- Persons of interest had bought various precious stones, precious metals and/or precious products (PSPMs), such as gold bars, luxury watches and jewellery.

It was also established that 109 foreign and Singapore companies were registered under the names of the persons of interest under investigation in this case. 66 companies were identified to be incorporated in Singapore. The companies were used to legitimise the persons of interest's stay in Singapore, enabling them to secure work passes, as well as open bank accounts to funnel illicit proceeds through.

- Two CSPs and their Registered Qualified Individuals who had facilitated the incorporation of 18 companies, were subsequently investigated and had their registrations cancelled for non-compliance with their AML/CFT obligations.

Singapore is actively sharing information through global law enforcement networks, including seeking assistance on the whereabouts of wanted persons, three of whom have INTERPOL Red Notices issued against them (as of May 2024), as well as sharing of information with relevant supervisory counterparts. STRO has also leveraged existing information exchange sharing arrangements with other financial intelligence units to spontaneously share relevant financial intelligence and send requests for assistance that could be helpful for investigations by domestic LEAs. STRO has also disseminated analyses of actionable financial intelligence to various domestic agencies for possible enforcement or regulatory action against suspicious entities.

This case demonstrates the strength of Singapore's AML/CFT regime to detect and disrupt illicit activities, and our commitment to take firm and decisive action against ML at the whole of government level.

To ensure that our AML regime remains robust, an Inter-Ministerial Committee (IMC) has been established to review and identify other areas of Singapore's AML/CFT regime that can be strengthened. The IMC review consists of the following main areas:

- Prevent corporate structures from being abused by money launderers.
- Enhance FIs' controls and effective collaboration with each other and authorities to guard against and flag suspicious transactions.
- Enhance DNFBPs' ability to better guard against ML risks.
- Centralise and strengthen monitoring and sense-making capabilities across Government agencies to better detect suspicious activities.

Money laundering

6.2.12 LEAs have observed a global trend involving an increase in layering across multiple jurisdictions, as organised crime groups and professional money launderers become more sophisticated in the application of their laundering techniques. This refers to standalone ML with nexus to foreign predicate offences and are pursued independently without prosecuting the predicate offences. ML is the second highest offence cited in requests for assistance received by Singapore from foreign authorities. The following case study is an example of how illicit funds can be dissipated in a short period of time across multiple jurisdictions, including Singapore. Hence, swift international cooperation is increasingly vital for jurisdictions to effectively clamp down on transnational ML. Singapore authorities will

continue to remain vigilant against transnational ML and are firm in our commitment to work with our foreign counterparts on this front.

Case Study 5 – Swift action taken by CAD for a multi-jurisdictional ML case

In mid-2020, CAD received information that a total of US\$11 million had been fraudulently transferred out of a US bank account maintained by a foreign government authority within a span of two weeks. US\$4 million of the monies had gone into a Hong Kong bank account, before it was broken up into 10 smaller transactions, which were transferred into a Singapore bank account.

CAD immediately commenced a domestic ML investigation and seized the remaining balance of US\$317,000, which was found to be held by a Hong Kong incorporated company. Investigations further uncovered that a CSP had assisted the company to open a bank account in Singapore. Notwithstanding the fact that the bulk of the funds had already been further diverted overseas by the time CAD was alerted to the matter, CAD expeditiously established that the monies in the Singapore bank account had been dissipated via 39 outgoing transfers to over 33 different corporate entities across nine jurisdictions. CAD subsequently reached out to the relevant jurisdictions through international cooperation channels.

Since then, the seized monies have been successfully restituted.

- 6.2.13 ML cases are commonly observed to involve the misuse of legal persons, particularly shell companies, and the misuse of bank accounts, particularly for cross-border funds transfers. LEAs have observed more instances of syndicated laundering, including involving networks of Singapore-incorporated shell companies. The bank accounts of these companies would feature rapid pass-through transactions between accounts ultimately controlled by a few common individuals. The following case study shows how LEAs unravelled a network of Singapore-incorporated companies set up by CSPs allegedly used for ML.

Case Study 6 – Whole-of-Government (WOG) action taken to tackle a network of legal persons used for the laundering of scam proceeds

In the second half of 2020, CAD started to observe a spate of BEC scams targeted at foreign corporate victims, and where Singapore corporate bank accounts were used to receive the fraudulent proceeds. CAD initiated a deep dive network analysis and uncovered a large network of over 3,000 Singapore-incorporated shell companies, which were suspected to be receptacles waiting to be deployed for ML. These shell companies were observed to be created by a number of common CSPs.

CAD established that most of the victims were corporates based in the US, with a smaller number based in other parts of the world such as Australia and some European countries. The allegedly fraudulent funds were received in the Singapore bank accounts of some of these Singapore shell companies, and it was observed that a large proportion of these funds were transferred out to other corporate bank accounts in another country (Country X), within one or two days. In some instances, Singapore bank accounts belonging to companies incorporated in yet another country (Country Y) with no Singapore presence, were also used for such laundering activities. As of February 2021, Singapore had received more than 80 reports, involving at least US\$104.3 million, that can be linked to this network.

CAD flagged this case to the RTIG for WOG mitigation action. This triggered a joint project between CAD, MAS and relevant ACIP bank members, where specific intelligence and leads were shared with the banks for them to surface new leads and to conduct further analytics within their entities. The information sharing led to over 990 STRs filed by ACIP bank members, which were analysed and disseminated by STRO to CAD to augment investigations. Coupled with CAD's close relationship with the US authorities, as well as Singapore LEAs' ability to initiate immediate freezing actions, Singapore authorities had closely collaborated with banks to intercept about US\$53 million worth of fraudulent funds, including more than US\$20 million of incoming funds that were blocked through the banks' proactive identification of suspicious accounts.

Twelve individuals, who were either local directors and/or CSPs of 35 incorporated companies were charged for failing to discharge directors' duties and for abetting the directors in the offences. As of May 2024, 6 of the accused persons have been convicted and each sentenced to an imprisonment term of between 4 to 6 weeks or a fine of an amount between S\$4,000 to S\$57,000, and disqualification from acting as a director of between 3 to 5 years.

ACRA had also conducted investigations and/or inspections on the CSPs involved. Two RFAs and two RQIs had their registrations cancelled by ACRA and 6 RFAs were imposed financial penalties ranging from \$4,000 to \$14,000 for breaches of their AML/CFT obligations. Through ACRA's analysis, ACRA shared information with CAD on an additional 25 individuals who were linked to the case, which had not surfaced in CAD's investigations.

To alert the broader industry and raise awareness, CAD, MAS and ACIP issued an ACIP advisory on this emerging typology involving professional ML and misuse of legal persons. MAS and ACRA have also subjected relevant banks and CSPs to more intensive supervisory scrutiny.

Corruption

- 6.2.14 The Transparency International Corruption Perceptions Index 2023 has found that the Asia-Pacific region poses significant corruption risks. Through projects participated in by relevant authorities in Singapore, it was further established that the threat of corruption proceeds being laundered within the Asia Pacific region (including Australia and New Zealand) is high. Neighbouring countries, such as Malaysia and Indonesia, have assessed corruption to be of higher threat within their jurisdictions²⁶. Taking these report findings into consideration and given Singapore's geographical location and standing as an international business, financial and trading centre, foreign corruption poses a higher ML threat to Singapore. In engaging various jurisdictions as part of the ML Threat Assessment, several countries stated that foreign corruption posed a material ML threat. Notably, some of these jurisdictions are in the Southeast Asia region.
- 6.2.15 Corruption is the third highest offence cited in incoming foreign requests to Singapore, with a large proportion of requests made via formal channels. The ML threat from foreign corruption is further amplified by the quantum of illicit proceeds from foreign corruption related ML cases investigated, which is significantly larger than the amount involved for domestic corruption related ML investigations.
- 6.2.16 The laundering of foreign corrupt proceeds in Singapore has been observed to involve a mix of self and third-party laundering, which may be facilitated by professional intermediaries

²⁶ Malaysia NRA 2017, Indonesia NRA Updated 2020

such as banks and CSPs. Corporate bank accounts set up by shell and front companies that have been incorporated by CSPs have been observed to have been used to layer foreign illicit proceeds from corruption, including through flow-through transactions under the guise of legitimate business transactions, where inflows of funds were then quickly transferred out of Singapore. There were also instances where foreign corruption proceeds were converted into private real estate in Singapore. An example of how CSPs were being misused by foreign criminal elements to launder criminal proceeds is seen in the case study below.

Case Study 7 – Individuals investigated for facilitating the setup of shell companies which have been misused for ML

CPIB investigated a case involving the suspected laundering of foreign corruption proceeds through Singapore bank accounts held by Singapore shell companies. The setting up of these shell companies and their banks accounts were facilitated by a CSP, which was set up by the accused on behalf of their foreign customers. Using the CSP as a front, the accused would also procure nominee directors for the companies and would instruct these directors to open accompanying corporate bank accounts. Thereafter, access to operate these bank accounts via internet banking credentials and the security token would be handed over by the CSP to the foreign customers. On some occasions, the accused acted as the nominee director himself.

In total, 13 nominee directors were found to have been used to create 54 shell companies for the CSP's foreign customers. Flow-through transactions amounting to approximately US\$3 million and EU€5 million were observed to be transacted through the Singapore bank accounts of two of the shell companies created via this scheme. Assistance from foreign authorities and FIUs were sought via international cooperation channels. However, there were no further leads to suggest that the nominee directors or the shell companies investigated were involved in ML activities. Eventually, prosecution was initiated against six nominee directors, including the accused person who set up the CSP for cheating offences and all six were convicted, with the most recent conviction in January 2024. The registration of the CSP involved was cancelled for AML/CFT breaches in 2021.

Tax crimes

6.2.17 Singapore is an international business, trading and financial centre and is one of 29 systematically important financial centres in the world. It intermediates cross-border transactions via a well-developed and efficient network and is a leading wealth management hub for the region. As at end 2022, total assets managed by Singapore based asset managers amounted to S\$4.9 trillion, with 76% of Singapore's assets under management originating from outside Singapore.²⁷ As a wealth management hub, Singapore is inherently exposed to ML involving tax crime proceeds originating from abroad. In engaging various jurisdictions as part of the ML Threat Assessment, some countries also raised tax offences as a predicate crime which posed a ML threat to Singapore.

6.2.18 Singapore has seen an increase in the number of incoming foreign requests relating to tax offences, via mechanisms such as MLAs, requests via STRO and INTERPOL. STRO further observed from an analysis of tax crime related STRs, that typical reasons for filing such STRs included customers being traced to adverse news and/or customers being involved in foreign tax amnesty programmes. Based on cases which LEAs have identified, LEAs have also observed that legal persons and arrangements could play a role in the laundering of foreign tax crime

²⁷ 2022 Singapore Asset Management Survey, MAS.

proceeds, where complex ownership and control structures could be used to hold funds/assets via bank accounts and/or other products. Professional intermediaries such as trust companies and asset managers may also be misused, as illustrated in the following case study.

Case Study 8 – Cooperation with foreign authorities to tackle an ML case arising from foreign tax evasion

CAD and MAS are looking into allegations against a Singapore licensed trust company (LTC X). LTC X had allegedly conspired with asset managers based in Country Y to set up complex trust structures for Person Z, a citizen of the US, with the aim of concealing Person Z's BO over certain financial assets.

This investigation arose from an MLA request from the US authorities, who had commenced civil forfeiture proceedings against Person Z. Person Z faced a tax evasion charge under the US laws for failing to declare assets in undisclosed and untaxed offshore bank accounts held outside the US.

LTC X had facilitated the setup and administration of two trust structures comprising companies A and B incorporated in Country C and was registered as the trustee of the assets under the trust structures. Companies A and B maintained corporate bank accounts in Singapore. From 2012 to 2017, Person Z routed his undeclared financial assets from a foundation in Country D to the said corporate bank accounts.

Working closely with the US authorities and leveraging financial intelligence referred by STRO, CAD seized S\$3.5 million from the corporate bank accounts. Pursuant to a settlement agreement between the US authorities and Person Z, the proceeds of the US tax evasion offences were recovered and eventually returned to the American government. Probes into ML offences and regulatory breaches of MAS' AML/CFT requirements by LTC X are ongoing.

- 6.2.19 LEAs leverage financial intelligence and other information sources including those from foreign counterparts to tackle and investigate into complex ML more effectively. The following case study demonstrates how financial intelligence disseminated by STRO led CAD to commence ML investigations and swiftly seize illicit assets arising from a foreign tax crime.

Case Study 9 – Financial intelligence-initiated investigations involving foreign tax evasion

STRO received an STR filed against Person A, a homemaker, whose source of wealth was derived from her divorce settlement from her former husband, Person B. Person B's source of wealth was allegedly derived from his career in a hedge fund company, Company C, where he was a hedge fund manager and held a senior position. Information from the STR indicated that Company C's bank account was reportedly used as a conduit to receive and transfer proceeds relating to foreign tax evasion.

STRO noted that Country D was investigating an alleged fraud of more than EU€22 million, involving Persons A, B and other entities. The fraud was in relation to the refund of dividend withholding tax charged by Country D. In particular, Person B was named as the main representative of the pension funds that raised applications to obtain withholding tax refunds. STRO then sent a spontaneous exchange of information on Person A to the FIU of Country D.

As the information that STRO had suggested that an ML offence involving foreign tax evasion may have been committed in Singapore through Person A, STRO analysed and disseminated the findings to the relevant domestic LEA. This led to the commencement of an ML investigation in Singapore, and the seizure of approximately GB£12.9 million and US\$7.9 million in monies and securities from Person A in Singapore. Investigations established that Person A is the beneficial owner of a trust in Singapore that fully owns Company C.

Investigations have concluded after establishing that no offence in Singapore was disclosed, due to the inability of the Country D authorities to provide sufficient evidence suggesting that the properties in question are tainted. A part of the seized assets has been returned to the foreign tax authorities in Country D following a settlement agreement reached between them and Person A.

TBML

- 6.2.20 Singapore is one of the busiest ports in the world in terms of shipping tonnage, with an annual average of 140,000 vessel calls. As an international financing, trading and transportation hub, Singapore faces an inherent threat of foreign TBML.²⁸
- 6.2.21 Whilst international trade, owing to significant volume and value, remains an attractive medium for money launderers to transfer large values across borders, TBML has also evolved to include exploitation of trade financing transactions.²⁹ In recent years, Singapore has seen an increase in the number of requests from its foreign counterparts relating to TBML activities with a Singapore nexus. Through engagements with jurisdictions, some countries have also provided feedback that TBML remains a key concern, in relation to ML typologies associated with Singapore.
- 6.2.22 Given the wide-ranging TBML typologies reflected in regional and international typology reports, it is noted that TBML cases can vary in complexity and could involve the exploitation of a range of sectors. Less complex TBML cases may be facilitated by shell or front companies, when false or forged trading documents are provided to third-party professional intermediaries, such as banks or accountants, to justify particular money flows. On the other hand, more complex cases may entail a mix of TBML techniques such as phantom shipments with multiple invoices, and/or the movement of actual goods to give the transaction a veneer of legitimacy. In addition to the misuse of shell/front companies, bank accounts and/or accounts, such complex cases could also involve the exploitation trade facilitators such as customs brokers or freight forwarders.
- 6.2.23 Inputs from ACIP³⁰ suggest that the majority of international trade finance transactions are carried out by banks under “Open Account” terms, where banks often have limited visibility over the underlying transaction. As TBML is often intertwined with trade finance processes, the banking sector may be a potential conduit used to layer illicit proceeds. A complex TBML case study involving the exploitation of shell companies to deceive banks into disbursing trade financing loans is depicted below.

Case Study 10 – TBML involving the misuse of shell companies to deceive banks into disbursing trade financing loans

²⁸ Singapore Financial System Stability Assessment; IMF Country Report No. 19/224; June 24, 2019

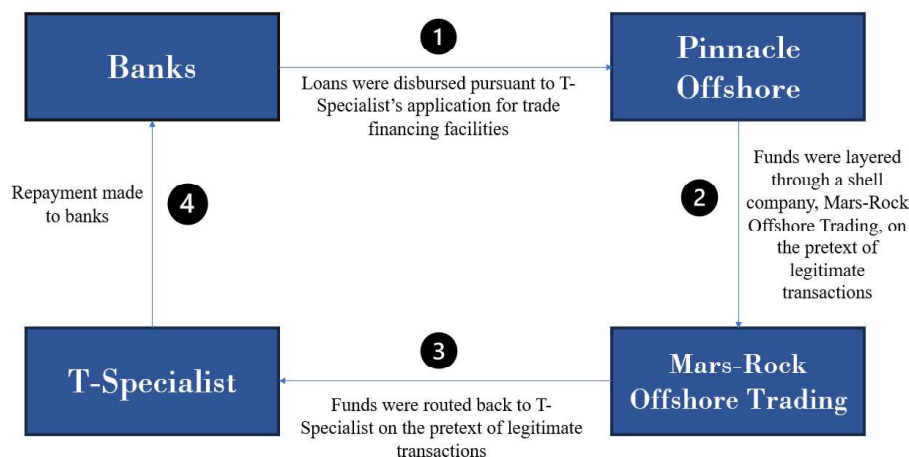
²⁹ FATF Trade-Based Money Laundering Trends and Developments; December 2020

³⁰ Please see ACIP Best Practices for Countering Trade Based Money Laundering <https://abs.org.sg/docs/library/best-practices-for-counteracting-trade-based-money-laundering.pdf>

After receiving foreign intelligence on illicit procurement networks involving the Democratic People's Republic of Korea (DPRK), CAD initiated investigations into potential PF offences committed by persons in Singapore. CAD's investigation was supported by STRs filed on relevant entities of interest.

Arising from cash flow issues, Ng Kheng Wah, the director of Singapore incorporated company, T-Specialist International Pte Ltd ("T-Specialist"), devised an invoice financing fraud to generate liquidity for the company. Ng Kheng Wah used 81 fictitious invoices purportedly issued by Pinnacle Offshore, a company incorporated outside Singapore, to T-Specialist to deceive five banks in Singapore into granting more than US\$95 million³¹ in trade financing loans to T-Specialist for the supply of non-existent goods.

Proceeds from the fraud were first disbursed from the five banks to Pinnacle Offshore, a shell company. The proceeds were then layered through Mars-Rock Offshore Trading, another shell company incorporated outside Singapore, and which maintained a bank account outside Singapore. Eventually, Mars-Rock transferred the illicit proceeds to T-Specialist and other companies under Ng Kheng Wah's control.



To give the banks the impression that the transactions were genuine, evidence of trade between Pinnacle Offshore, Mars-Rock Offshore Trading and T-Specialist, such as false trade documents/invoices were created and shown to the banks.

Further, when the banks disbursing the trade financing loans to Pinnacle Offshore requested for shipping documents to evidence the movement of goods, T-Specialist falsely informed the banks that Mars-Rock Offshore Trading had delivered their goods to Pinnacle Offshore by road, and hence that there were no shipping documents (e.g. bills of lading/airway bills) available. In fact, no goods were shipped at all, and the banks had no other means of verifying the movement of the goods based on open-source databases.

In 2019, Ng Kheng Wah was convicted of fraud offences, whilst T-Specialist was convicted of ML offences. Apart from the above-mentioned offences, Ng Kheng Wah and T-Specialist were also convicted for PF offences. Ng Kheng Wah, through T-Specialist, had supplied prohibited luxury items

³¹ Equivalent to approximately S\$128.4 million.

exceeding S\$6 million to a departmental store chain in the DPRK, in breach of UN sanctions against DPRK. Ng Kheng Wah was sentenced to an imprisonment term of 34 months and T-Specialist was sentenced to a total fine of S\$880,000.

- 6.2.24 International typologies note that storage facilities are used to store high-value cultural objects, and such storage facilities may represent ML/TF vulnerabilities.³² In Singapore's context, the Free Trade Zones (FTZs) are used largely for intermittent storage of sea containers and other goods pending transshipment. In this regard, Singapore has assessed the risks of the FTZ and implemented risk mitigation measures such as a legal requirement for FTZ operators to report on suspicious activities as well as for warehouses as FTZ cargo handlers, to report on any goods suspected to be in contravention of written law. Please refer to the Annex on Singapore's FTZ Regime for more information on these risk mitigation measures.
- 6.2.25 Located outside of Singapore's FTZ are commercial storage facilities and warehouses which store high-value goods such as precious stones and precious metals, antiques, works of art and watches clad with precious metal casings or precious metals (referred to as listed goods) with Goods and Services Tax (GST) suspended under Singapore Customs' licensing scheme. For example, Le Freeport that opened in 2010 is a commercial storage facility whose tenants are allowed to store such goods with GST suspended if the tenants are licensed by Singapore Customs to operate a Zero GST Warehouse (ZGW). Le Freeport operations are outside of Singapore's FTZ. Tenants which do not store any GST-suspended goods in Le Freeport do not require a licence from Singapore Customs. Singapore does not grant any special facilitation to Le Freeport. There are also other ZGWs licensed by Singapore Customs to store GST-suspended listed goods located outside of Le Freeport.
- 6.2.26 As listed goods are prone to ML/TF risks due to their high values and relative ease of transfer, it was reviewed that these four types of goods should be regulated more tightly. From 2018, in order to further enhance the oversight of ZGWs storing listed goods, ZGW licensees are required to seek approval from Singapore Customs prior to storing the listed goods in their ZGWs. All such applications from ZGWs to store listed goods will be assessed by Singapore Customs on a case-by-case basis. ZGWs are required to meet more stringent requirements before they may be approved to store listed goods, as they would have been assessed to have better internal controls and compliance levels.
- 6.2.27 In addition to obtaining and maintaining details and values of the listed goods, ZGWs are also required to maintain and update information on the identity of the person(s): (i) who deposited the goods, (ii) with control over the goods, and (iii) with beneficial ownership of the goods. ZGWs are also mandated to screen these persons against publicly available databases for relevant criminal activities and to file a Suspicious Transaction Report (STR) in the event of a positive result. Singapore Customs conducts regular checks and audits to ensure that ZGWs abide by these requirements and maintain and update the necessary information.
- 6.2.28 In 2019, to strengthen the regulatory regime on ZGWs storing listed goods, Singapore Customs further mandated ZGWs storing works of art and antiques to obtain, maintain and update information on the name of the works of art or antique, name of artist, dimensions, and the last transaction date.

³² FATF report on Money Laundering and Terrorist Financing in the Art and Antiquities Market (2023)

6.3 DOMESTIC ML THREATS

- 6.3.1 Singapore's major ML threats, derived from predicate offences committed in Singapore, are fraud, criminal breach of trust and UML.

Fraud, particularly Cyber-enabled Fraud

- 6.3.2 Fraud remains as Singapore's top crime type based on conviction figures. Specifically, the number of cyber-enabled fraud increased by 46.8% from 31,728 in 2022 to 46,563 in 2023. The total amount lost from cyber-enabled fraud amounted to S\$651.8 million in 2023.³³
- 6.3.3 The cyber-enabled fraud situation in Singapore has been exacerbated by Singapore's increasingly digital savvy population. High internet penetration, rising digital literacy and the ease of access to financial systems in Singapore have contributed to more residents interacting and transacting online. The proportion of households with online expenditure increased from 31.3% in 2012 to 2013, to 60% in 2017 to 2018.³⁴ This trend has intensified owing to the social distancing measures put in place during the Covid-19 pandemic, as more residents stayed home and transacted online. Such an environment has led to the rising trends in cyber-enabled fraud cases seen locally.
- 6.3.4 In 2020, the Inter-Ministry Committee on Scams (IMCS) was formed for a more holistic approach towards tackling the cyber-enabled fraud situation in Singapore. As part of the IMCS, CAD works closely with MAS and the Association of Banks in Singapore (ABS) to enhance the payment ecosystem in Singapore. CAD and MAS recognise that cyber-enabled fraud pose an ML risk to Singapore as some scam victims also act as money mules, facilitating the movement of illicit proceeds both within and through Singapore. The IMCS continues to proactively undertake measures to mitigate the cyber-enabled fraud situation in Singapore, including disrupting the supply of money mules in Singapore.
- 6.3.5 A large proportion of the cyber-enabled fraud in Singapore has a foreign nexus and is perpetrated by foreign criminal syndicates. Referencing INTERPOL reports, financial fraud is a fast-evolving threat in the Asia region, where countries were found to be prime targets of financial fraud given their position among the fastest growing digital economies in the world. Specifically, LEAs have observed an increase on two fronts. There is an uptick in the use of both individual and corporate money mules in Singapore to layer/receive and transfer scam proceeds out of Singapore. LEAs have also seen more instances where money mules in Singapore were recruited/created by overseas syndicates to receive and launder proceeds from cyber-enabled fraud and/or other fraudulent activities occurring overseas. This is similarly supported by our engagements with jurisdictions – based on intelligence and investigations, several jurisdictions have received illicit funds from Singapore either arising from fraud occurring in Singapore or having passed through Singapore.
- 6.3.6 With better understanding of the threat and nature of cyber-enabled fraud, Singapore has devoted significant resources to strengthen our capabilities to contain and limit the perpetration of cyber-enabled fraud within and beyond Singapore as much as possible through the set-up of ASC (that eventually evolved to ASCom), and by working closely with other jurisdictions.

³³ Please see SPF Annual Scams and Cybercrime Brief 2023

³⁴ <https://www.singstat.gov.sg/-/media/files/publications/households/ssn219-pg1-5.pdf>

Case Study 11– Network of money mules in Singapore used to launder proceeds for foreign syndicates

In late 2021, Singapore was hit by a series of phishing cyber-enabled fraud involving spoofed SMS messages, and in some of the instances, actual and look-alike sender-IDs of local banks were used. In one of the series, more than S\$13.7 million was lost, affecting 790 victims. The fraudsters involved are typically part of organised criminal syndicates and run sophisticated transnational operations which are not easy to detect or dismantle. The syndicates are also well-resourced and adept at using technology to cover their tracks.

Thus far, 121 local bank accounts and 89 overseas accounts have been identified to have received proceeds of the fraud. In one instance, the money mules recruited in Singapore were promised a fixed salary of \$3,000 a month, with an additional \$600 to \$800 for each bank account provided to the syndicates in Telegram chat groups between Dec 2021 and Jan 2022.

The unauthorised transactions were made to money mules with local bank accounts. Typically, after the funds were received in the local mule's account, they would be (i) withdrawn in cash via ATM, (ii) transferred to another local bank account, (iii) transferred to overseas accounts, or (iv) used to top up e-wallets. The scam proceeds were eventually transferred out of Singapore to other countries.

Nine persons were charged for their involvement in this case. As of May 2024, seven of them have been convicted of offences under the CMA, Penal Code and CDSA and, depending on their level of involvement, were given sentences ranging from 18 months' supervised probation and reformatory training to 15 months' imprisonment.

- 6.3.7 LEAs have observed extensive methods to launder fraudulent proceeds which cut across multiple sectors in Singapore. The sectors involved have evolved over time, as criminals tend to be opportunistic and agile in exploring new laundering techniques. It is noted that the fraudulent proceeds leave Singapore within a very short span of time, layered across jurisdictions.
- 6.3.8 While cyber-enabled fraud proceeds are frequently observed to be laundered through individual and corporate bank accounts as well as through cross-border money transfer service providers, LEAs have also observed emerging conduits for laundering, such as through digital payment tokens (DPTs) and gift cards. The Police have observed cases where the victims were deceived into using their fiat currency to purchase DPTs. These DPTs were traced to various private wallets, and at times, cryptocurrency exchanges. Singapore has also seen instances where money mules were recruited by perpetrators under the pretext of job advertisements, to purchase gift cards from convenience stores in Singapore after receiving deposits in their bank accounts. The deposits were actually inflows of criminal proceeds from victims. The mule would then receive a commission for providing the unique serial number/pin of these gift cards to the perpetrator through online means.
- 6.3.9 On the other hand, LEAs have also observed that proceeds arising from fraud cases (non-cyber type) may be withdrawn and held in cash or layered through the purchase of high value assets such as private real estate and PSPMs. The following case study shows how proceeds derived from a fraud case were laundered through multiple conduits, including bank accounts belonging to shell companies, as well as through the use of cash and PSPMs.

Case Study 12 – Multiple sectors misused for the laundering of proceeds from domestic fraud

Between 2017 and 2019, 12 persons were prosecuted under the Companies Act, Penal Code and Computer Misuse and Cybersecurity Act³⁵ as well as under the CDSA for ML offences, for their involvement in the largest complex public fraud seen in Singapore thus far. Four key members of the syndicate fled Singapore before investigations commenced. Through close collaboration with key foreign counterparts to track their whereabouts, CAD managed to locate and repatriate all four members back to Singapore for prosecution.

The syndicate was found to have used eight companies and one partnership to create the impression that three training institutions had delivered training to more than 25,000 individuals. The public agency was thus falsely induced into disbursing S\$40 million in false claims to the bank accounts of these legal persons. The majority of the illicit proceeds were laundered through cash withdrawals from corporate accounts.

Ng Cheng Kwee, a key member of the syndicate, enlisted his spouse, Lee Lai Leng, to help him conceal a portion of the proceeds, which he handed to her in cash. In turn, Lee Lai Leng converted a total sum of S\$626,500 into gold bars through cash purchases at two PSMDs as directed by her husband. The couple then hid these PSPMs and a further S\$6.7 million of illicit cash proceeds in Lee Lai Heng's brother's home. The latter played an active role in concealing these illicit proceeds by moving them to a friend's home for safekeeping. Andy Quek, another member of the syndicate had also used his criminal proceeds to purchase jewelry of approximately S\$28,000 from a PSMD in cash. In all, illicit proceeds/assets valued at approximately S\$18 million were seized in the course of investigations.

All 12 persons have been sentenced to imprisonment, ranging from terms of between 33 months and 213 months for this matter. The three PSMDs were also found to have failed to submit cash transaction reports (CTRs) and were prosecuted and convicted accordingly. One of the three PSMDs was additionally convicted of failing to perform its requisite customer due diligence obligations. The three PSMDs were issued with fines of between S\$9,000 and S\$40,000.

Criminal Breach of Trust

- 6.3.10 Criminal breach of trust (CBT) remains a key domestic ML threat for Singapore, augmented by the propensity for large sums of illicit proceeds to be laundered from the crime. CBT has consistently been identified as one of the key predicate offences prevalently committed in Singapore. Having said that, the modus operandi for CBT is generally less syndicated in nature and is observed to typically be perpetrated by lone criminals who abuse their positions of power or responsibility. As such, LEAs have observed more self-laundering arising from CBT.
- 6.3.11 Criminals who perpetrate CBT are observed to generally be more educated or resourceful, and consequently, capable of adopting a range of laundering methods. The incidence of CBT offending has remained stable across the years, affirming that the offence is more opportunistic in nature, and is less likely to be influenced by external environmental factors. The following case study shows how laundering of large amounts of criminal proceeds from CBT was conducted by the predicate offender through cash withdrawals, remittances and to fund his gambling activities.

³⁵ The Computer Misuse and Cybersecurity Act has since been renamed the CMA on 31 August 2018, following the operationalisation of the Cybersecurity Bill.

Case Study 13 – Heavy gambler convicted of CBT and ML charges

Person A was employed as an accounts clerk of a Singapore incorporated company. The company had been appointed to manage the operations and financial affairs of several offshore companies, and Person A was assigned to handle the bookkeeping and payment functions for these companies. STRO found suspicious transactions by Person A that were not commensurate with his income, including large cheque payments from various companies in 2013, and referred actionable financial intelligence to domestic LEA for investigation.

Between January 2007 and March 2014, Person A misappropriated the equivalent of S\$46.2 million from the offshore companies' Singapore bank accounts. He used cheques or telegraphic transfer forms pre-signed by the BOs of the bank accounts to make cash withdrawals or to transfer funds to his personal bank accounts.

Person A was a heavy gambler and used the criminal proceeds to fund his gambling activities, which ranged from placing bets with Singapore Pools to gambling at the casinos. In 2019, Person A was convicted and sentenced to 18 years' imprisonment for CBT and ML.

Case Study 14 – Employees siphoning marine fuel from a petroleum refinery

In 2018, 52 persons were arrested for their involvement in siphoning marine fuel from a petroleum refinery in Singapore. Investigation revealed that between August 2014 and January 2018, a total of 438 incidents of theft were committed which amounted to over 365,000 metric Tonnes (mT) of fuel. The market value of the stolen fuel is approximately US\$174 million.

Juandi Pungot ('Juandi') was among the arrested and identified as one of the masterminds who conspired to misappropriate marine fuel from the petroleum refinery. As a former employee of the refinery, he admitted to having partaken in the conspiracy since 2007. Between August 2014 and January 2018, he misappropriated up to 203,403 tonnes of marine fuel worth S\$128 million.

To cover their tracks, Juandi and his conspirators also bribed six independent surveyors who signed off on the volumes of fuel transfers to vessels.

Juandi pleaded guilty to 20 counts of CBT, six corruption charges for bribing six independent surveyors to turn a blind eye to the misappropriation and 10 other CDSA charges for laundering his criminal proceeds. He was sentenced on 31 March 2022 to a total of 29 years' imprisonment, one of the longest prison terms for a commercial crime.

Unlicensed Moneylending

- 6.3.12 UML is a longstanding problem for Singapore. UML borrowers are driven by a plethora of reasons to take out loans from unlicensed moneylenders. The allure of quick and easy access to funds attracts borrowers who are desperate for money but cannot secure loans from licensed institutions for various reasons, such as having poor credit ratings due to many unpaid outstanding loans, and/or not meeting the minimum income requirements. Some may also need quick cash to settle an urgent financial need and were not able to provide or were deterred by the controls and documentation required by licensed institutions. Unlicensed moneylenders often target vulnerable individuals and offer them quick financial

solutions but at an exorbitant interest rate. Nonetheless, there is another group of UML borrowers that have emerged in recent years. This group of borrowers had genuinely mistaken the unlicensed money lenders as licensed after finding them via various social media platforms or receiving unsolicited messages from them; or were ‘forced’ to take up the loan after they made enquires with the UML thinking that they were a legitimate business. For the latter, the UML would transfer them the loan amount, or partial amounts, without their consent and subsequently demand exorbitant interest payment.

- 6.3.13 UML activities are often operated by multi-tiered syndicates with overseas nexus, resulting in a high propensity for UML proceeds to be laundered across borders. The transnational nexus for UML activity has become more prominent as many UML ringleaders have been forced to shift their operations outside of Singapore to avoid apprehension as a result of heavy legislative punishment and active Police intervention. While the UML ringleaders are predominantly based overseas in the Asia-Pacific region, their underlings continue to carry out UML activities in Singapore. As a result, UML cases largely involve third-party ML perpetrated by syndicate underlings.
- 6.3.14 Monies funding the UML business in Singapore are believed to be transferred into Singapore bank accounts from abroad, and held as “float money”, before being transferred to borrowers as loans. UML syndicates typically disburse loans and receive repayments via different debtors’ bank accounts to prevent detection. The syndicates would instruct the debtors to repay their loans by making bank transfers to mules or other new borrowers, making it harder to trace the fund back to the syndicates. The Police has also observed borrowers turning to assisting the syndicates by ceding control of their bank accounts to the syndicates, passing their automated teller machine (ATM) card and/or relevant details of their bank accounts to the syndicates in order to reduce their debts. Some may even open new bank accounts and hand over access to the accounts to the syndicates in lieu of payments for their debts. The Police has also observed an emerging trend where an increasing number of persons who have no ties to UML or any criminal syndicates are seen selling their banking credentials online to buyers for financial gains. Often, UML criminal syndicates would buy over their banking credentials and use them for illicit activities. The first case study is an example of someone working as an UML ATM runner and using an ATM card ceded to the UML to perform UML-related activities; while the second case study showcases a financial-intelligence initiated investigation against a subject who relinquished banking credentials simply for financial gains.

Case Study 15 – Misuse of ATMs to perform electronic bank transfers by UML syndicates

Person A had borrowed from an unlicensed moneylender due to personal financial difficulties. Sometime in January 2022, he faced difficulty in keeping up with the repayments, and accepted the UML syndicate’s offer to work as an “ATM runner” for the syndicate to reduce his debt. Person A was tasked to collect ATM cards of bank accounts ceded for use to the syndicate and used the cards to perform relevant electronic bank transfers for the syndicate. Person A was charged with 18 counts of assisting an unlicensed moneylender in a business of moneylending and sentenced in December 2022, to six months’ imprisonment. He was also fined S\$150,000.

Case Study 16 – Financial-intelligence initiated investigation involving relinquishment of banking credentials for financial gains.

In September 2023, STRO received an STR filed against Person A, for having voluminous suspicious transactions that resembled a UML typology. The STR was referred to the Police for further investigation.

Investigation revealed that Person A had received a Telegram message from an unidentified person asking if she wished to earn fast cash. When she made queries, she was offered a monthly payout of \$200 if she relinquished her bank account. She accepted the offer and handed over the internet banking token linked to her bank account to the unidentified person.

The bank had seen a high volume of transactions from August 2022 to 5 April 2023 thereafter the bank proceeded to close the bank account due to the high volume of suspicious transactions.

In March 2024, Person A was charged in court for one count of offence under the CMA for relinquishing her bank account which was eventually used to facilitate the flow of illicit proceeds. Prosecution against Person A is currently in progress.

- 6.3.14 Most of the illicit proceeds generated from UML are handed over in cash to money mules responsible for physically transporting the cash overseas to the UML ringleaders. Given travel restrictions due to the Covid-19 pandemic, a reduction in the physical transportation of monies across borders has been observed. Instead, the syndicates are believed to be using remittance services to move their ill-gotten gains overseas, by disguising the monies as legitimate business dealings with overseas counterparties, including through the use of shell companies. The Police have also observed illicit proceeds from UML being 'moved' out of the country without monies actually moving across border. They make use of the "hawala" system to bypass the traditional banking systems. This system is based on mutual trust and the balancing of hawala brokers' books. In this case, it consists of a network of moneychangers located around the globe. Between the network partners, no formal contract or paperwork is involved in the monetary transactions.

Case Study 17 – ML through hawala system and money changer

In 2022, the Police conducted an operation targeted at members of an unlicensed money laundering (UML) syndicate. It was found that the director of a local money changer, Person A had assisted a money changer based in Country M to dispense monies to UML runners and also receive criminal proceeds from UML runners.

Investigations revealed that Person A had assisted with at least 13 of such illegal transactions, each ranging between S\$10,000 to \$30,000. Person A has been charged with CDSA offences and prosecution is in progress.

- 6.3.15 The Police coordinate regular island-wide enforcement operations against bank account holders found to have relinquished control of their bank account for UML purposes or simply for financial gains; or have assisted unlicensed moneylenders to perform banking transactions to launder illicit monies. The Police and FIs would work closely to ensure that bank accounts with suspicious transactions linked to UML activities are proactively frozen for their suspected UML involvement. This is part of ongoing efforts by the Police to keep a close rein on the UML situation, its offenders and to curtail the misuse of the banking system. Recognising that the bank accounts are most misused for UML, upstream intervention measures have also been

established to prohibit persons convicted or warned of UML offences from possessing ATM/internet banking facilities for a one-year period upon the conclusion of their UML case.

Environmental Crime

6.3.16 Environmental crimes, including illegal wildlife trade, illegal logging and illegal waste management, are transnational crimes that converge with other crimes such as corruption, threaten biodiversity and/or have significant negative impact on economies. Given Singapore's position as an international financial centre, trading and transport/transshipment hub, Singapore is vulnerable to illicit flows from Environmental Crime and related ML. Singapore has thus separately published a targeted risk assessment on Environmental Crime ML on 29 May 2024 to raise the financial and DNFBP sectors' awareness of this risk.³⁶

Other criminal threats of interest

Cybercrime

6.3.17 In the context of this NRA, cybercrime refers to cyber-dependant crime which are offences investigated under the Computer Misuse Act (CMA) such as ransomware, hacking and website defacement. The growth of cybercrime is a global phenomenon, particularly exacerbated in recent years by the rapid digitalisation across Asia due to the Covid-19 pandemic. The need for remote work and online services during the pandemic drove significant technological advancements in Singapore, catalysed by its Smart Nation initiative, increased digital inclusivity and high internet penetration. As an international financial hub with high financial connectivity, Singapore benefited from the pandemic-driven digital advancement. However, this progress also led to an increase in cybercrime and cybersecurity challenges as digitalisation reshapes the means of communication and business operations³⁷ and provides more opportunities for the commission of offences under the CMA. The Cyber Security Agency of Singapore (CSA) has reported seeing an increase in cybercrime over the past few years.

6.3.18 Singapore has responded to this growing threat by strengthening its existing legislation and criminal justice framework to deal with cybercrime threats. For example, Singapore introduced the Online Criminal Harms Bill in July 2023, which empowers authorities to deal more effectively with online activities that are criminal in nature³⁸. In May 2023, the CMA was also amended at the same time to prevent the abuse of Singpass for criminal activities. The amendments to the CMA criminalises the act of sharing Singpass credentials without proper verification, and to obtain or deal in Singpass credentials unless for lawful reasons.

6.3.19 LEAs note that cybercrime is one of the top proceeds generating offences internationally. Notwithstanding that cybercrime may be conducted to cause disruption or for the purpose of cyber espionage (i.e. non-profit motives) and despite having generated some volume of monetary losses from victims in Singapore in recent years, the scale remains under control.

6.3.20 Among the cyber-dependant crimes, ransomware is noted as a potential growing ML threat in Singapore. As a large amount of illicit money is involved in a ransomware payment, criminals

³⁶ <https://www.mas.gov.sg/news/media-releases/2024/singapore-issues-environmental-crimes-money-laundering-national-risk-assessment>

³⁷ Please see channelnewsasia.com/news/singapore/cybercrime-hacking-phishing-online-crimes-covid-19-15178948 and channelnewsasia.com/news/singapore/cybercrime-jumps-more-than-50-2019-new-threats-covid-19-csa-12872818

³⁸ MHA press release on 8 May 2023 – Introduction of the Online Criminal Harms Bill (mha.gov.sg)

might make use of Singapore's financial hub to launder their illegal proceeds. Since 2018 there has been an upward trend in the number of ransomware cases reported, albeit there was a slight dip of 4% in 2022, with 132 cases reported.³⁹ While there are currently no money laundering cases arising from ransomware attacks in Singapore, it remains a potential ML threat and measures have been taken to address this risk.

- 6.3.21 Singapore has established the Counter-Ransomware Task Force (CRTF), to bring together government agencies across relevant domains to strengthen Singapore's counter-ransomware efforts and to push for international action against the global ransomware threat. CSA is also closely monitoring local developments in ransomware attacks and working with international counterparts on collective efforts to counter the global ransomware threat. The following case study shows an example of how ransomware can cause disruption to business, as well as the challenges faced in money tracing by the authorities and the ease of laundering illicit proceeds in the cyber realm by criminals.

Case Study 18 – Ransomware Strain

In 2022, Person A, who is the owner of company X, was informed by the staff that their company's mobile application was unable to connect to the server. The IT support team, who was activated to provide assistance later discovered that some of the servers were encrypted with ransomware. The ransomware strain was believed to be the Caley ransomware since all the encrypted files extension were ".caley". The perpetrator demanded a Bitcoin payment of 0.4 BTC and eventually settled for 0.25 BTC after negotiation.

Person A subsequently made payment to a given address of a BTC wallet. As a result, the perpetrator then emailed Person A the decryption key. Following that, everything went back to normal after decryption was done.

Investigation revealed that the money trail involved multiple hops, such as the use of mixers and through freelance traders before it reached a centralised exchange based overseas. Funds were transferred to a cryptocurrency mixer, which mixes potentially identifiable cryptocurrency funds with others so as to obscure the trail back to the fund's original source, making attribution of the eventual outflow of funds to the user difficult.

- 6.3.22 Overall, there are currently low incidences of ML cases arising from CMA offences in Singapore, and these cases mostly involve self-laundering, as illustrated in the following case study. Nonetheless, based on international reports, it is anticipated that more complex CMA offences may ensue, particularly where criminal syndicates are involved, and these cases may involve more third-party laundering. Such criminal syndicates are also expected to launder monies through more sophisticated means, as they are more capable of exploiting IT loopholes.

Case Study 19 – Self laundering arising from computer misuse crimes

Person A was sentenced to six months' imprisonment for CMA and ML offences in 2018. As an accounts officer of an insurance company, Person A was in charge of processing cheques for maturity payments and claims for policyholders. Under the pretext of issuing cheques to policyholders, Person A logged into his company's internet banking account and amended 16 cheques to reflect himself as the payee instead. He then credited the cheques which amounted to

³⁹ CSA website – Ransomware portal <https://www.csa.gov.sg/Tips-Resource/ransomware-portal>

approximately S\$88,000 into his personal bank account. Subsequently, he laundered a portion of the proceeds by remitting them to Country X through a payments cross-border money transfer service company in Singapore.

Drug-related offences

- 6.3.23 The ML threat in relation to drug trafficking needs to be closely tracked even though Singapore has remained a relatively drug free society. Singapore's status as a financial hub, makes us vulnerable to the movement of drug crime-related illicit funds in and through Singapore, especially since we are a reputable financial centre near the 'Golden Triangle'. The CNB is also aware of the presence of active transnational organised groups supplying drugs to Singapore. CNB enjoys a close working relationship with foreign counterparts and has instituted many joint operations to deal with drug syndicates, including extradition to Singapore to face criminal charges.
- 6.3.24 Cash couriers for drug syndicates may make use of cross-border money transfer services providers and money changers to launder their illicit proceeds. Syndicates may also seek to launder illicit proceeds by converting their illicit proceeds to PSPMs (e.g. gold), or via the real estate sector to purchase properties. This would be consistent with the modus operandi of syndicates operating in other countries in the region, e.g. Thailand and Malaysia⁴⁰. From the cases we have observed and investigated, they relate more to cases where most of the proceeds are still in the possession of the trafficker (self-laundering). Should investigations reveal that the financial assets are derived from drug proceeds, regardless of whether the subject had been prosecuted and/or convicted of a drug ML offence, CNB would proceed with the forfeiture and disposal of the financial assets under the relevant legislations, thereby depriving and preventing the subjects from being unjustly enriched. This is one of the key tenets in Singapore's overarching framework of dealing with organised crimes.
- 6.3.25 While there have been no cases of foreign drug ML, CNB is cognisant that the illegal narcotics industry is a transnational problem. Hence, CNB has been an active participant and leader, working closely with regional and international counterparts to tackle this issue. CAD and CNB continuously and proactively check with their foreign counterparts for further information to conduct investigations and render assistance to them where necessary. In addition, CNB also proactively scans international and regional reports for mentions of any illicit drug and drug funds flow into or out of Singapore and would conduct follow-up checks with foreign counterparts on the said report.

Domestic Organised Crime

- 6.3.26 As an international business, financial and trading centre, Singapore recognises its exposure to organised crime and its consequent laundering threat. The Organised Crime Act (OCA) enhances Singapore's ability to disrupt the activities of organised criminal groups at various levels of their hierarchy and prevent them from establishing a foothold in Singapore to perpetrate serious crime.
- 6.3.27 Between 2016 and 2023, Singapore saw more than 40 convictions under the OCA. These convictions typically related to complex cases involving a large number of syndicate members

⁴⁰ Based on engagements with counterparts in other jurisdictions, it was established that drug-related money laundering could be carried out through cash, vehicles, properties, jewellerys, expensive watches etc.

as well as high value seizures. As an example, the seizure for one of the OCA cases amounted to more than S\$35 million, confirming the increased ML threat arising from organised crime to Singapore. Given the quantum of illicit proceeds involved, criminals are also expected to launder their monies through more sophisticated methods, including across borders. LEAs observed that the real estate and banking sectors are more vulnerable to the ML threat of organised crime. LEAs have lodged caveats against private real estate properties in Singapore, traced to proceeds from organised crime, which have taken place in Singapore. The following case examples illustrates some ML methodologies used by organised crime groups to launder crime proceeds.

Case Study 20 – Organised crime and ML

In 2016, Police commenced investigations targeted at illegal online betting websites facilitating lotteries involving persons from various levels of an organised crime group.

Ow Choon Bok ('Ow') operated an illegal online lottery betting business in Singapore between 2010 and 2016 by receiving lottery bets, collecting, disbursing cheques and cash related to the remote gambling activities. Between 2010 to 2016, Ow had transferred illegal proceeds amounting to approximately S\$133,000 to his former employer for the purpose of making contributions towards his account under the Central Provident Fund, as the banks would consider that as a relevant factor when assessing his loan applications.

Apart from offences under the OCA, Remote Gambling Act and Common Gaming House Act, Ow was also charged for ML offences for transferring the benefits in cash to his employer over multiple occasions. His employer then topped up his Central Provident Fund, as part of "employer's contributions"⁴¹. Eventually, he was convicted and sentenced to eight months' imprisonment for the ML offence.

Confiscation proceedings were initiated under the CDSA against Ow upon his conviction. On 27 July 2022, the Singapore High Court issued a confiscation order of about S\$1.25 million against him. The realisable properties included bank balances, security holdings as well as a landed property.

Case Study 21 – Organised crime and ML

In 2018, Police commenced investigations targeted at public gaming activities involving persons from various levels of a secret society group.

Ho Hong Seng ('Ho') belonged to one of the secret society groups and he was involved in running illegal public gaming stalls since 2015. The syndicate recruited him as a croupier and operator for their gaming stalls. In 2016, Ho also started to operate his own public gaming stalls with his group. His proceeds of crime were either deposited into his bank accounts or used to purchase one luxury watch at about S\$11,600.

Aw Teck Huat ('Aw') belonged to another secret society group, and he was the turf controller of the illegal public gaming stalls since 2015. He would recruit other operators, stall lookouts and stall

⁴¹ The Central Provident Fund is Singapore's mandatory social security savings funded by contributions from employers and employees. Employers in Singapore are required to contribute to their employees' CPF accounts via monthly CPF contributions, under certain conditions. There was insufficient evidence to prove ML for the employer in the case study.

assistants to help him with his gambling den. He also supplied unsold bread from his own bakery business to the operators of the illegal public gaming stalls and received the payments from them.

Apart from offences under the OCA, Common Gaming House Act and Societies Act, Ho was also charged for ML offences such as converting a sum of S\$11,600 into a luxury watch and concealing casino chips worth over S\$250,000. Eventually, Ho was convicted and sentenced to 21 months' imprisonment. The luxury watch, cash, and monies in his bank accounts with a total value of about S\$82,000 were forfeited to the State.

Aw was charged for the offences under the OCA, Common Gaming House Act, Societies Act, and ML offences such as converting criminal proceeds into about S\$600,000 of casino chips and acquiring about S\$148,000 that are believed to represent benefits from criminal conduct. He was convicted and sentenced to 20 months' imprisonment. The cash and monies in his bank accounts with a total value of about S\$20,000 were forfeited to State.

Domestic tax-related offences

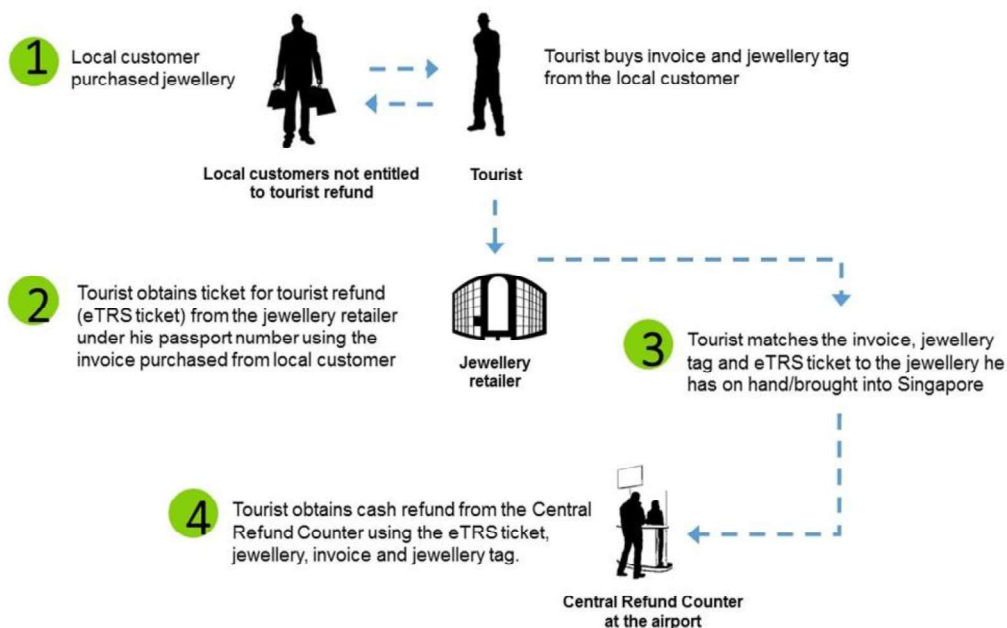
6.3.28 In recent years, Singapore has seen 15 convictions relating to syndicated cases of fraudulent Good and Services Tax (GST) refund claims under the electronic tourist refund scheme (eTRS)⁴². These syndicates were observed to typically remove the criminal proceeds out of Singapore after extracting the refunds fraudulently from the eTRS. The following case study is an example of a syndicate convicted for eTRS fraud and ML offences.

Case Study 22 – Syndicate convicted for fraudulent GST refunds and ML

Five foreigners were convicted in 2017 for engaging in a conspiracy to claim fraudulent GST refunds at Changi Airport Singapore, and consequently removing the illicit proceeds from Singapore. Joint operations by IRAS and Singapore Customs revealed that fraudulent GST refund claims of approximately S\$167,000 were made by the five accused persons since 2015. A graphic illustration of the fraudulent GST refund claim is shown below:

⁴² Please see <https://www.iras.gov.sg/irashome/GST/Consumers/Tourist-Refund-Scheme/>

Illustration of a Tourist Refund Fraud



CAD's parallel financial investigations revealed that the syndicate had removed criminal proceeds amounting to almost S\$113,000 from Singapore. Each of the syndicate members eventually faced over 200 charges for fraudulent GST refund claims and a total of 127 ML charges. They have each been convicted and sentenced to between 38 and 39 months' imprisonment for both fraudulent GST refund claims and ML charges. They were also subjected to court fines ranging from S\$14,000 to S\$70,000, and tax penalties of about S\$52,000 which was 3 times the tax undercharged.

- 6.3.29 To tackle the emergence of eTRS fraud, IRAS has imposed more stringent requirements on specific retailers assessed to be more susceptible to syndicated eTRS fraud activities. For example, such retailers are required to pack their goods that have been purchased in tamper proof, serially numbered and sealed bags to prevent goods tampering and to implement closed-circuit television (CCTV) surveillance systems at their retail premises. IRAS also uses data analytics and other tools to improve its capabilities to detect non-compliance with these requirements and fraudulent GST refund claims. This serves to deter fraud, and to facilitate IRAS' efforts in fraud detection.
- 6.3.30 More recently, IRAS has also observed emerging complex and syndicated Missing Trader Fraud (MTF) schemes which were used to perpetrate GST refund fraud. Syndicates orchestrating these MTF schemes would create a network of businesses involving shell companies and/or use a network of front companies with genuine business activities to create a façade of bona fide business activities within the supply chain. IRAS has observed that most of these business activities conducted by the syndicates were done with the sole aim of fraudulently extracting GST refunds from the Singapore government. The GST refunds were observed to be most frequently laundered via bank accounts in the name of these shell and front companies and/or their associated entities.
- 6.3.31 As of 31 March 2024, IRAS has determined that more than 450 GST-registered businesses audited by IRAS are suspected to be involved in MTF in Singapore, and the quantum of fraudulent GST refunds amounted to approximately S\$265 million.

Case Study 23 – Prosecution of individuals involved in the use of a shell company to perpetrate MTF involving approximately S\$114 million of fictitious sales

Between February 2015 and January 2016, a Singapore-incorporated GST-registered company, Company N, purportedly sold high-value electronic goods amounting to approximately S\$114 million to various businesses. GST was charged on these sales. Company N is alleged to be a shell company without genuine business operations and was used to generate purchase orders and sales invoices to support subsequent GST refund applications by exporters. IRAS received claims in GST refunds amounting to close to S\$8 million, arising from sales purported to be generated by Company N.

Four men were alleged to be behind Company N's fraudulent operations. Each has been charged for being a knowing party to a fraudulent business, and for the forgery of sales invoices. A fifth man has also been charged for allegedly assisting individuals who were operating Company N, to commit forgery, while a sixth man was charged for his role in being the nominee director of Company N.

Additionally, a seventh man, the director of two Singapore incorporated GST-registered companies, Company O and Company P, has been charged for his alleged involvement in falsification of accounts. He is alleged to have facilitated the fraud by allowing the two companies to purchase non-existent goods from Company N.

The nominee director of Company N was sentenced to a fine, while five of the other six men have been sentenced to imprisonment of between five and 63 months. Court proceedings for one man are still ongoing.

- 6.3.32 Overall, the number of convictions relating to domestic tax-related crimes has remained low. Since the inclusion of tax offences as serious offences under the CDSA in 2013, Singapore has also seen a few ML prosecutions and convictions arising from tax-related predicate offences. This is indicative of Singapore's continued vigilance and enforcement against tax crimes. Singapore will continue to monitor the evolving typologies of tax crimes to develop effective countermeasures. The following case study shows how financial intelligence shared by STRO with IRAS led to an investigation and successful conviction of a case involving domestic tax evasion.

Case Study 24 – Financial-intelligence initiated investigation involving domestic tax evasion

STRO's analysis detected a STR that was indicative of possible tax evasion and referred the matter to IRAS for investigation. The STR revealed numerous cash deposits amounting to more than S\$1 million into Person A's bank account over a period of four months, which Person A had claimed to be earnings from her pub establishments.

Acting on the STR, IRAS initiated an investigation into Person A. Investigations later revealed that Person A was the controlling mind and the sole decision maker for the business operations of two pub establishments, even though Person A was not listed as a shareholder or director.

Person A had orchestrated an arrangement to omit the cash sales from the two pub establishments' income and GST declaration. The pub establishments were found to have made false entries in their Income Tax Returns and correspondingly, understated output tax in their GST Returns.

Person A was convicted of assisting two pub establishments to evade Income Tax and GST. As a result, Person A was sentenced to 41 weeks' imprisonment and ordered to pay tax penalties and fines amounting to over S\$2.3 million.

6.4 CONCLUSION OF KEY ML THREATS

- 6.4.1 As an international business, financial and trading centre with an open economy, Singapore is inevitably exposed to the threats of complex transnational ML, including by criminal syndicates and professional criminal elements seeking to use Singapore as a transit or integration point to launder illicit funds from abroad. In particular, authorities have observed a greater ML threat to Singapore from predicate offences committed abroad, ranging from fraud, organised crime, corruption and tax to TBML. Singapore also faces ML threats arising from UML and CBT, albeit to a lesser extent. Authorities in Singapore have observed a wide variety of laundering techniques being used. Shell companies are observed to be among the vehicles most commonly used by foreign elements to obscure their identities to facilitate illicit activities. Illicit funds could be layered across multiple financial and DNFBP sectors, before being integrated or further layered. The ease and speed with which money and assets can move across borders today means that enforcement agencies and regulatory authorities must cooperate and coordinate even more swiftly and extensively, in order to deprive criminals of the benefits of crime and to take them to task for their wrongdoings.
- 6.4.2 While Singapore faces a low domestic crime rate, we are not spared the global surge in ML threats posed by fraud, particularly cyber-enabled fraud. STRO and the Police have observed that the syndicates are often based overseas, and that the fraudulent proceeds are often laundered across several jurisdictions (including Singapore) within a short span of time. We continue to be cognisant of the threats posed by cyber-enabled fraud, the range of sectors that such criminals seek to exploit, such as banks, DPTSPs, and other payment service providers, and the abuse of individual and corporate mules in these typologies.
- 6.4.3 The assessment of threats is a continuous and dynamic process, and we also continue to vigilantly monitor the ML threats posed by other crime types of interest, including environmental crime, cybercrime, drugs-related offences, domestic organised crimes and domestic tax-related offences.

7. SECTORAL RISK ASSESSMENTS – FINANCIAL SECTOR

7.1 OVERVIEW

- 7.1.1 Singapore has been ranked by the IMF as one of 29 systematically important financial centres in the world. Singapore's financial centre is dominated by banks and intermediates cross-border transactions via a well-developed and efficient network. Singapore currently hosts more than 1,000 FIs, which offer a wide variety of financial products and services and serve a broad and diverse customer base.
- 7.1.2 As an international business, financial and trading centre with an open economy, Singapore is inevitably vulnerable to the risks of complex transnational ML, including by syndicated and professional criminals, seeking to use Singapore as a transit, integration or destination point for laundering of illicit funds from abroad. Authorities in Singapore have also observed a wide range of laundering techniques being used in Singapore, including complex and syndicated ML involving the use of bank accounts and payment accounts, structures such as shell companies, trusts and other complex structures, and which span multiple jurisdictions and sectors.
- 7.1.3 Taking into account the (i) extent of exposure to the ML threats, including Singapore's exposure to known regional and international ML typologies, as well as other information derived from investigations, and intelligence obtained from foreign counterparts, STRs, MLAs, and RFAs, (ii) vulnerability of the entities in the financial sector to ML, and (iii) strength of the entities' AML/CFT controls, the assessed ML risks of these entities are summarised in the table below. The detailed ML risk assessments are set out in the following sections.

High ML risks	Banks
Medium High ML risks	DPTSPs Payment Institutions <u>with</u> Cross Border Money Transfer Services Licensed Trust Companies (LTCs) External Asset Managers (EAMs)
Medium Low ML Risks	Fund Management Companies (excluding External Asset Managers) Money Changers Payment institutions <u>without</u> Cross-Border Money Transfers Broker Dealers and Corporate Finance Advisory Firms Moneylenders
Lower ML Risks	Non-Bank Credit Card Companies Approved Trustees Finance Companies Direct Life & Composite Insurers Securities Depository Insurance Brokers Financial Advisers

- 7.1.4 Overall, the banking sector has been identified as posing the highest level of ML risk within the financial sector, while DPTSPs and payment institutions conducting cross-border money transfer services, LTCs, and EAMs have been identified as posing relatively higher levels of ML

risk within the financial sector. In particular, illicit funds flowing into or through Singapore are observed to be most commonly laundered via bank accounts, particularly as rapid pass-through transactions involving cross-border fund flows, and generally through the use of third parties such as mules. Both corporate and individual mule bank accounts have been observed to be typical conduits exploited by money launderers, particularly where foreign criminal syndicates and professional money launderers are involved. Where corporate mule accounts are observed, they generally involve the misuse of shell companies, including networks of Singapore-incorporated shell companies ultimately controlled by a criminal network for ML purposes. The bank accounts of these companies would be misused, and illicit proceeds could be channelled into or through Singapore under the guise of legitimate business transactions. In some instances, illicit funds have also been withdrawn in cash or remitted overseas through the use of cross-border money transfer service providers.

7.2 FINANCIAL SECTOR ANTI-MONEY LAUNDERING REGULATORY AND SUPERVISORY FRAMEWORK

- 7.2.1 Singapore's approach is to develop a comprehensive and sound legal, institutional, policy and supervisory AML/CFT framework. The CDSA is the primary legislation in Singapore which criminalises the laundering of criminal benefits by both natural and legal persons and provides for the investigation and confiscation of such benefits. It also requires the reporting of STRs by all persons, including FIs, in Singapore.
- 7.2.2 In addition to the CDSA requirements, FIs regulated by MAS are required to comply with MAS regulations, which impose AML/CFT obligations on our FIs pursuant to sections 15 and 16 of the Financial Services and Markets Act 2022 (FSMA).
- 7.2.3 The specific requirements and expectations on FIs are set out in the relevant MAS' AML/CFT Notices, Guidelines and other guidance documents. These AML/CFT requirements are wide-ranging and include customer due diligence (CDD), enhanced customer due diligence (ECDD) for higher risk customers, ongoing monitoring, record keeping, STR reporting etc. These requirements are regularly reviewed and updated to ensure alignment with standards set out and updated by relevant global bodies such as the FATF, and with the changing risks faced by Singapore⁴³.
- 7.2.4 MAS assesses and screens prospective FIs and their key personnel (i.e. substantial shareholders, beneficial owners, board of directors and key appointment holders) to ensure that we only admit and license institutions and individuals that meet MAS' fit and proper criteria. The assessment is comprehensive and covers a range of factors including (i) their financial soundness, source/adequacy of capital and business plans; and (ii) AML/CFT-related factors such as adverse news, previous sanctions, strength of the applicant's head office's AML/CFT controls, track record with home supervisor and compliance with FATF and global regulatory standards. FIs also require MAS' approval for any changes in controlling interest, board of directors and key appointment holders. Prior to its approval, MAS will conduct screening and background checks with various sources, including with LEAs, internal and commercial databases and foreign supervisors. This prevents unfit persons such as criminals from taking a significant or controlling interest or holding a management position in Singapore's FIs.

⁴³ For example, on 3 November 2020, MAS announced the discontinuation of the issuance of the S\$1,000 note from 1 January 2021. This was a pre-emptive measure to mitigate potential ML/TF risks associated with large denomination notes and is aligned with international norms. MAS had earlier ceased issuance of S\$10,000 notes in 2014.

- 7.2.5 MAS adopts a dynamic and surveillance led risk-based approach (RBA) to its supervision of its FIs, where supervisory attention is informed by our risk surveillance insights and prioritised on key/emerging ML/TF risk triggers and thematic risks as well as higher risk FIs. MAS considers a range of information and tools to assess ML/TF risks in the financial sector, which informs its supervisory interventions. This includes analysis of risk indicia based on information collected from FIs. Information collected includes data on each FI's cross-border activities, exposures to cross-border funds flows to/from higher risks countries, the profile of their customer portfolio, trade finance volume etc. MAS enriches this information with information from other sources such as STRs, domestic/foreign intelligence from LEAs and supervisors, industry partnerships, and material adverse media.
- 7.2.6 MAS strives to continuously improve and refine its risk surveillance and assessment framework to ensure that it remains relevant and effective. MAS has been building and applying data and network analysis to improve its risk surveillance capabilities, to better detect higher risk activities and FIs in the financial system. These techniques are applied over a range of data, including the aforementioned risk assessment metrics, STRs⁴⁴, business registration information, FI transactional data etc. MAS is also developing its next-generation analytics platform, which will consolidate its data sources into a single platform for holistic analysis and incorporate more advanced analytics capabilities, including machine learning. This would lead to more effective identification and assessment of risks.
- 7.2.7 The use of data analytics, coupled with information from other sources and intelligence from domestic and foreign supervisory and law enforcement counterparts, has enabled MAS to identify concerning networks of bad actors and activities, and to pro-actively target FIs handling transactions presenting potentially higher ML, TF and PF risk concerns for more intensive supervisory scrutiny. This has enabled supervisors to act more quickly, and be more risk targeted in identifying material control deficiencies or thematic risk concerns that require prompt attention.
- 7.2.8 MAS has a range of supervisory intervention tools to address and mitigate ML/TF risks and threats identified. The range of tools include the use of circulars and advisories to quickly alert FIs to new risks or typologies, the conduct of supervisory engagements/inspections to address specific or thematic risks and concerns as well as the use of external auditor reviews to complement our supervisory assessments.
- 7.2.9 Thematic risk areas covered by MAS in recent years include, among others, transaction monitoring, foreign tax evasion risks and corruption risks related to politically exposed persons (PEP), PF risks, risks involving the misuse of legal persons and complex structures, and TBML. MAS shares key observations from its thematic engagements, emerging typologies and useful case studies with the industry, to enhance their risk awareness and AML/CFT practices. In this regard, MAS has issued several guidance papers and circulars to set out supervisory expectations in these thematic areas and higher risk sectors, such as for private banking, EAMs, LTCs and DPTSPs.
- 7.2.10 Proportionate and dissuasive sanctions are applied to FIs that have been found to have breached their AML/CFT requirements and/or their officers who have fallen short of their duties. Between 2018 and 2023, MAS had taken actions against 17 FIs for breaches of

⁴⁴ In line with STRO's enhancement of SONAR, MAS worked with STRO to ensure that STRs filed by financial institutions are now directly piped into MAS' systems. This facilitates analysis and allow MAS to better detect networks across STRs.

AML/CFT requirements. These actions range from revocation of licence, financial penalties to reprimands. For serious breaches, MAS has also issued prohibition orders against officers of the FIs, which prohibit them from conducting regulated activities and/or acting as management, directors or substantial shareholders of FIs. Lifetime bans have been imposed for egregious cases.⁴⁵ To raise industry awareness and serve as further deterrent, MAS also publishes on our website the enforcement actions taken for more serious breaches or against errant FIs and officers.

7.2.11 MAS has been strongly encouraging FIs to develop their data analytics capabilities. Such capabilities will allow them to process large amounts of data and uncover anomalies in transactions or customer behaviours more effectively, enabling better detection of bad actors. Over the past few years, MAS has observed an increased adoption of data analytics techniques for financial crime purposes amongst the FIs, especially the banks.

7.2.12 MAS also leverages the ACIP and relevant industry associations (such as the Singapore Trustees Association, Association of Crypto Currency Enterprises and Start-ups Singapore) to collaborate with the industry to identify risks and drive risk understanding, assessment and mitigation across the system. For example, ACIP had set up a number of working groups, comprising a range of experts across the industry, to look into key industry risk concerns such as the misuse of legal persons and TBML, and to explore the use of data analytics to combat financial crime. MAS had also collaborated with the Singapore Trustees Association to develop a best practices paper on managing ML/TF risks associated with complex trust structures.⁴⁶ These products also fed into the NRA process.

Box Story 1 – MAS and CAD’s Collaboration with banks through ACIP

ACIP is co-chaired by MAS and CAD and comprises a Steering Group of nine banks and ABS. ACIP brings together stakeholders from the financial sector, regulators, LEAs and other government agencies to collaboratively identify, assess and mitigate key and emerging ML, TF, and PF risks facing Singapore.

Since it was established in 2017, ACIP has become an effective platform for collaboration between government and industry and has proven effective in the identification and promotion of focal areas to uplift the implementation of AML/CFT measures in Singapore.

The ACIP Steering Group is supported by various expert working groups to study identified areas of interest. For example:

- the Risk Surveillance working group which allows MAS, CAD and banks to exchange information and assessments, to mitigate emerging risk typologies, including those related to high-risk corridors of transnational fund flows as well as emerging higher risk activities or indication of risk transfers.
- the Legal Persons and Arrangements working group which works with MAS, CAD and ACRA on measures to strengthen the industry’s understanding of risks associated with the

⁴⁵ Please refer to MAS’ Enforcement Report, which provides updates on enforcement matters in the financial markets and highlights key outcomes and outlines MAS’ enforcement priorities. The report is published once every 18 months. The latest Enforcement Report 2022/2023 covers the period between 1 January 2022 to 30 June 2023 (<https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/mas-enforcement-report-2022-2023>).

⁴⁶ Please see: [Industry-Best-Practice-Paper-Managing-ML-TF-Risks-Associated-with-Complex-Trust-Structures.pdf \(sta.org.sg\)](#)

misuse of legal persons and arrangements (including the use of complex structures, front and shell companies and other arrangements).

- the Digital Assets Risk Management working group which provided guidance to banks to understand and manage ML, TF, and PF risks arising from customer relationships with nexus to digital assets.

Over the years, ACIP has issued best practice papers⁴⁷ to recommend measures that banks and other FIs can take to identify, prevent, and disrupt illicit financial activities. For timelier information sharing, “ACIP Advisories” were introduced in April 2019 to allow quick dissemination of risk information on significant cases and typologies observed by MAS, CAD, other government agencies or ACIP members, to the industry. The advisories alert industry to new and/or emerging risks, including those relating to legal persons and complex structures, tax fraud, professional ML etc., so that industry (and not only ACIP members) can take swift measures to mitigate these risk concerns.

Example of typologies identified through ACIP:

Macro-fund flows: Through macro level monitoring of payment flows and network linked analysis, ACIP banks detected a significant increase in fund flows from jurisdictions bordering or linked to Country X which is subject to sanction measures. These spikes were observed during the period following escalations in geopolitical tensions, occurring in a flow-through manner to companies based in Aisa and the Middle East. While the link between these funds and specific criminal activities is not apparent, the disproportionately large and unexplained volumes of flow-through transactions from these geographical regions, lack of clear economic rationale, and the shell-like characteristics of the entities involved raised concerns that the transactions could reflect attempts at evading sanctions imposed by various jurisdictions. An ACIP Advisory was issued to alert industry to the diversion of Country X-related payments via third party jurisdictions.

Virtual Accounts: Through information sharing among member banks, ACIP has uncovered instances where the product offering of “virtual accounts”⁴⁸ by banks to Payment Service Providers (PSPs) has been misused in novel ways. There were instances where front and/or shell companies opened payment accounts with the PSPs and these PSPs utilised “virtual accounts” provided by the banks to facilitate reconciliation of payments made to their clients’ accounts. In some instances, these PSPs offered other PSPs the use of these virtual accounts. From the banks’ perspective, funds sent to the front/ shell company’s payment account with the PSP are credited into the bank account of the PSP via the virtual account, without a direct relationship entered into between the bank and the PSP’s clients. The ML risks are heightened in situations where CDD measures to detect potential front/shell companies could be inadequate, as LEAs have observed that proceeds paid to virtual accounts held by such front and/or shell companies were illicit proceeds. An information note was prepared and circulated by ACIP to alert the rest of industry to various risks pertaining to virtual accounts, and mitigation measures that can be and have been undertaken.

⁴⁷ For example, Legal Person – Misuse Typologies and Best Practices (May 2018), Best Practices for Counter Trade-Based Money Laundering (May 2018), Industry Perspectives – Adopting Data Analytics Methods For AML/CF (Nov 2018), Industry Perspectives on Best Practices – Management of Money Laundering, Terrorism Financing and Sanctions Risks from Customer Relationships with a Nexus to Digital Assets (Jul 2023), Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risks Associated with Receiving Referrals from Corporate Service Providers (Feb 2024), Industry Perspectives on Best Practices – Leveraging on DA and ML Methods for AMLCFT (Mar 2024).

⁴⁸ Virtual Accounts refer to services offered by banks which enables the bank’s customers to reconcile payments made in relation to customers of the bank’s customers. Unique “virtual accounts” numbers are assigned to the customers of these bank’s customers and payments are allowed to be made to these virtual accounts.

Since 2019, CAD and MAS have also worked on specific cases with ACIP bank members, under the Case Specific Investigation (CSI) framework. Intelligence and leads are shared by CAD with ACIP banks through a “hub and spoke” model, where the banks can conduct further analytics on the information received and then provide feedback in the form of new leads to CAD. The cases involved key ML threat concerns such as the misuse of legal persons to receive and/or launder illicit proceeds, including from overseas sources. Collaboration between CAD, MAS and the banks led to the detection, investigation and successful prosecution of cases as illustrated in the case example below. Further, ACIP’s efforts have also facilitated LEAs’ successful interception of about US\$ 53 million, including more than US\$ 20 million of incoming funds that were blocked through the banks’ proactive identification of suspicious accounts (refer to Case Study 6 above for more details).

Case example – Agritrade International Pte Ltd

In 2019, an ACIP bank alerted CAD on Agritrade International Pte Ltd (“Agritrade”)’s under invoicing, phantom shipments and suspected use of shell companies. CAD commenced CSI with the banks, where the banks filed STRs relating to Agritrade to STRO. STRO subsequently analysed the STRs and disseminated the relevant information to CAD, allowing CAD to take swift and effective action.

With the financial intelligence from ACIP CSI, and multiple reports lodged by banks and finance companies who had extended credit facilities to Agritrade for the purposes of trade financing, CAD commenced investigations into the former Chief Financial Officer (“CFO”) of Agritrade in January 2020.

In January 2023, the former Agritrade CFO was convicted of 11 counts of cheating under Section 420 of the Penal Code, Cap 224 (“PC”) and 1 count of falsification of accounts under Section 477A of the PC. She was sentenced to imprisonment of 20 years for deceiving 16 financial institutions of more than US\$469 million.

ACIP will continue to pursue the following key objectives (i) identify and tackle key priority risks/emerging risks; (ii) raise AML/CFT competencies and uplift key segments of the broader industry; and (iii) support the public-private collaboration in case-specific investigations.

- 7.2.13 As part of Singapore’s whole-of-society approach against the abuse of Singapore’s financial system for illicit purposes, MAS also closely coordinates its supervisory efforts with LEAs where criminal activities are suspected and with other supervisors where their supervised entities (e.g. companies service providers, lawyers, accountants) are involved. The coordination is done bilaterally or through the RTIG.

Box Story 2 – FIs’ controls and MAS’ reviews in relation to Singapore’s recent major money laundering case

In a recent major ML case, FIs detected suspicious activities and filed numerous STRs on the persons of interest, prior to the case breaking publicly. These STRs on the persons of interest and related persons were identified by the FIs’ transaction monitoring and in some cases, through the use of data analytics. In many instances, the FIs took additional precautions and actions, such as enhanced

monitoring and/or closing these individuals' accounts. The STRs enriched STRO's analysis and supported the subsequent actions by law enforcement agencies.

MAS had also identified networks of related STRs through our data analytics, and alerted STRO, LEAs and fellow supervisory agencies to similar criminal typologies through RTIG. MAS additionally alerted the industry to emerging risks observed, with a nexus to the recent case:

- In April 2022, MAS issued a circular to warn FIs of these emerging typologies and engaged the key FIs to tighten their controls.
- From 2022 to mid-2023, FIs also highlighted to ACIP risk concerns, typologies and information relating to concerning fund flows.

The close coordination between MAS, FIs and Police was instrumental when it came to the operation itself:

- MAS worked closely with Police and FIs to rapidly identify the tainted funds so the Police could seize these funds swiftly. This prevented the suspects from dissipating their ill-gotten gains. FIs also responded promptly to Police orders to produce information, which helped Police build their case against these suspects.

As additional information emerged from the operation, MAS was able to analyse the fund flows in our system better. This enabled us to prioritise our supervisory engagements and inspections on FIs with a major nexus to this case. STRO also disseminated relevant information through their analysis to MAS to facilitate MAS' supervisory actions against the FIs.

MAS is in the midst of the inspections, to ascertain whether FIs had performed adequate checks on the customers' sources of wealth and funds, applied appropriate enhanced checks and monitored customer transactions to pick out suspicious ones to file STRs promptly, and took reasonable steps to mitigate against ML/TF risks. Where there are breaches of AML/CFT requirements, MAS will take firm and proportionate actions.

To further strengthen the effectiveness of AML/CFT controls implemented across the financial sector, MAS will be providing additional supervisory guidance in some key areas including the following:

- conduct of customer risk assessment; and
- corroboration of customers' source of wealth/source of funds.

7.3 BANKS

Key exposures to ML threat areas

- 7.3.1 Banks in Singapore are regulated by MAS and offer a wide range of products and services such as deposit taking, providing cheque services and lending, across a broad spectrum of customer segments such as retail banking, private banking, corporate banking etc.
- 7.3.2 Singapore's analysis of known domestic, regional and international ML typologies indicate that the banking system is most commonly featured as being misused for ML purposes. Banks are also most prevalently featured in domestic ML investigations arising from both domestic and foreign predicate offences, foreign requests for assistance, STR filings as well as in incoming and outgoing MLAs. Hence, the ML threat for the sector is High.

- 7.3.3 Banks in Singapore have been exploited for a variety of ML typologies, such as self-laundering and third-party laundering, across the different stages of ML, from placement to layering and to integration. LEAs have further observed that individual bank accounts are more prevalently featured for domestic crime threats, whereas corporate bank accounts are more often exploited to launder proceeds from a range of foreign crimes.
- 7.3.4 Bank employees are well placed to discover and take advantage of any weaknesses in their organisations' internal controls. This contributes to the banks' overall risk, as bank officers may abuse their position to defraud their clients and launder the proceeds. LEAs and MAS have taken actions against such bank officers who violate the integrity of Singapore's financial system. An example is shown in Case Study 25.

Case Study 25

Low Taek Jho ("Jho Low") and his associates were alleged to have misappropriated more than US\$6.5 billion from 1Malaysia Development Berhad (1MDB), a Sovereign Wealth Fund based in Malaysia, and its subsidiaries. The criminal proceeds were believed to be used for the personal benefits of Jho Low and his associates and laundered through various bank accounts in Singapore and four other countries. In particular, at least US\$4 billion were allegedly laundered via multiple bank accounts maintained by at least six different banks in Singapore through the use of complex investment structures that were facilitated by professional intermediaries, such as bankers and overseas fund management companies.

Following the commencement of investigations, Singapore issued a warrant of arrest against Jho Low and issued an INTERPOL Red Notice against him. 3 bankers, namely Yak Yew Chee, Yvonne Seah Yew Foong and Jens Fred Sturzenegger were convicted for offences of failing to report suspicious transactions, forgery and giving false information to the authorities. They were sentenced to imprisonment terms of between 2 weeks and 29 weeks and fined between S\$10,000 and S\$128,000. Another banker, Yeo Jiawei was convicted for offences of witness tampering, money laundering and cheating charges and was sentenced to imprisonment of more than 54 months while another of his associate, Kelvin Ang Wee Keng was sentenced to a fine of S\$9,000 for one charge of corruption. Financial intelligence from STRO supported these investigations.

Singapore also investigated Goldman Sachs Singapore Pte (GSSP) and two of its former Managing Directors, Tim Leissner and Ng Chong Hwa (also known as Roger Ng), in relation to the three bond offerings underwritten by Goldman Sachs International for the subsidiaries of 1MDB. In October 2020, the SPF issued a Conditional Warning in lieu of prosecution to GSSP for the offences of corruption. Pursuant to the Conditional Warning, GSSP committed to, among other things, paying US\$122 million to the Singapore Government and another sum of US\$61 million to Malaysia.

Singapore has also seized bank accounts and curtailed the dealing of properties belonging to various individuals. As of May 2024, the Singapore Court has ordered the return of about S\$103 million of seized monies to Malaysia.

In addition, MAS had investigated and taken firm actions against FIs which failed to meet MAS' AML/CFT requirements. MAS took decisive steps to revoke the licenses of 2 banks (BSI Bank Limited and Falcon Private Bank Ltd, Singapore Branch), as well as imposed financial penalties totalling S\$32.8 million on 11 FIs. MAS also reviewed the conduct of officers of the FIs involved in this case and issued prohibition orders (POs) against 11 individuals (including the persons named above)⁴⁹.

⁴⁹ Please refer to MAS' website for more information on actions taken by MAS.

These POs prohibit the individuals from performing regulated activities and acting as directors or substantial shareholders in the financial sector, for a period ranging from three years to lifetime bans, taking into consideration their involvement in the case and severity of their misconduct.

- 7.3.5 The banking sector's ML threats are largely driven by the following factors:
- (i) Transnational crime syndicates exploiting the banking sector as a destination or transit point for the proceeds of crime (e.g. relating to syndicated fraud and scams, corruption etc.). This includes the misuse of complex legal (e.g. shell companies, sometimes through multiple layers) or financial structures to engage in business/trade finance transactions to receive/move illicit funds, evade tax or for PF purposes, including across borders;
 - (ii) As a leading wealth management hub, which serves both domestic and foreign high net worth individuals (HNWI) and PEPs, the sector (including private banks) is exposed to potential abuse by criminal elements seeking to hold/move proceeds, in particular, from foreign corruption or tax evasion; and
 - (iii) Emerging cybercrime threats, together with rapid developments in financial technology and the ubiquity of accessing banking services on the internet and smart mobile devices, which may have inadvertently created new opportunities and channels for ML.

Box Story 3 – Measures targeted at risk related to private banking and wealth management

Given the attributes of the clients in Private Banks (PBs) (which includes HNWI, PEPs etc), size and complexity of transactions, PBs pose inherently higher ML/TF risks, particularly in the areas of corruption and foreign tax-evasion. MAS has thus continued to focus on strengthening AML/CFT controls in PBs.

From 2019 to 2021, MAS conducted a series of thematic inspections on PBs, and identified areas which the PBs could improve in their AML/CFT controls. These included the need to improve oversight by senior management over corroboration of clients' Source of Wealth (SoW) and Source of Funds (SoF), and detection of suspicious funds flows. In 2020, MAS issued a guidance paper on effective AML/CFT controls in PBs, which sets out observations from the thematic inspections and emphasises MAS' supervisory expectations to raise the banking sector's risk awareness and understanding of AML/CFT controls. More recently in 2022 and 2023, MAS initiated another series of thematic follow-ups with and inspections of PBs, to address specific risk concerns in light of the increased demand for wealth management services in Singapore. Further guidance was issued by MAS to the wealth management sector to remind FIs to remain vigilant to ML/TF risks and ensure that their risk controls keep pace with the growth and developments of their wealth management business. Specifically, MAS highlighted the need to conduct quality assurance testing on key controls and continue to pay close attention to higher risk customers and transactions.

The wealth management sector includes LTCs and EAMs. Since 2018, MAS had conducted a series of inspections on and engagements with LTCs and EAMs. MAS also conducts regular townhalls and issued additional guidance to increase these FIs' risk awareness and strengthen their AML/CFT controls⁵⁰.

Apart from PBs, LTCs and EAMs, MAS has observed an increasing number of Single Family Offices (SFOs) being set up in Singapore to access investment and philanthropic opportunities here and in the broader Asian region. SFOs manage assets belonging to a family and are commonly used for wealth management purposes. FIs dealing with SFOs are thus required to understand related ML/TF

⁵⁰ MAS issued guidance papers on "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in 2019 and "Strengthening AML/CFT Practices for External Asset Managers" in 2022.

risks and ensure that AML/CFT controls are adequate to address these risks (including customer due diligence, and corroboration of the SoW/SoF of the SFOs and their beneficial owners). With the growth of SFOs in Singapore, MAS had proposed and consulted on additional measures to strengthen surveillance and defence against ML/TF risks posed by SFOs and is currently reviewing the feedback received.

Vulnerability Assessment

Sector characteristics

- 7.3.6 Overall, banks are assessed to be more vulnerable to ML. Singapore has a sophisticated and inter-connected banking system comprising over 150 banks. As at the end of 2023, the banking sector had a total asset size of almost S\$3.5 trillion. Singapore's banking sector provides customers with a wide range of accessible and efficient online financial services. As one of the world's international financial centres, Singapore is a hub for payment and settlement services and intermediates cross-border transactions via a well-developed and efficient network. Banks in Singapore offer a wide range of products and services and serve a broad spectrum of corporate and individual customers, both domestic and foreign. As such, they are correspondingly exposed to a diverse spectrum of customer risk. Banks feature commonly in domestic, regional and international ML typologies, and the high volume of banking activity in Singapore contributes significantly to its higher ML vulnerability.
- 7.3.7 Beyond size and cross-border transactions, the riskier nature of some banks' primary activities exacerbates the sector's vulnerability. Although banks in Singapore do not have a high proportion of customers from higher risk jurisdictions on an aggregate basis, the sector is highly sophisticated, with leading corporate and private banks offering a slew of complex financial products and advice to cater to the needs of businesses as well as HNWIs, both domestic and foreign. As one of the world's fastest growing wealth management centres, Singapore's banks also offer high-value private banking facilities and service a number of higher risk customers, such as PEPs. More complex products/structures may also be involved. While there are legitimate reasons to use these products and services, their complexity and, in some cases opacity, could lead to their misuse for ML/TF purposes such as for laundering of funds from foreign corruption and tax evasion.
- 7.3.8 Given the significant global role of Singapore's financial sector, banks in Singapore are susceptible to misuse via transactions or business activities with companies or structures (both domestic and foreign), often established with professional expertise. Shell and front companies have been observed to be misused for ML, foreign tax evasion, foreign corruption, and PF purposes. In particular, front companies pose greater challenges for banks given the comingling of legitimate and illegitimate funds within their transactions.
- 7.3.9 However, the overall cash intensity of the banking sector is relatively low, in line with the greater digitalisation of banking services in Singapore and is not a major driver of the sector's vulnerability. A potential area of emerging vulnerability, however, is the online-only "digital banks". In December 2020, MAS awarded four digital banking licences to non-bank players, who are subject to the same AML/CFT requirements as "traditional" banks. These new entrants may bring innovative practices, including in the field of AML/CFT, to the sector. Conversely, their novel business models and potential lack of familiarity with the banking sector and AML/CFT may also increase the sector's ML vulnerability.

- 7.3.10 Internationally, cybercrimes are known to evolve rapidly, making continued cooperation, and sharing of experience on such crimes a necessity. Singapore has an increasingly digital savvy population with over 99% of households having access to the internet and over 94% of individuals who are internet users. Rising digital literacy and greater digitalisation of banking services have made Singapore's banking sector more susceptible to cybercrimes involving cyber-enabled fraud and data theft incidents (e.g. from phishing, malware etc.).

AML/CFT controls within the sector

- 7.3.11 Banks in Singapore are licensed under the Banking Act and are required to comply with MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism and its accompanying guidelines. These include requirements to conduct CDD, ECDD for higher risk customers such as PEPs and to establish their source of wealth and source of funds via appropriate and reasonable means, perform transaction monitoring, maintain records and to file STRs.
- 7.3.12 Due to the scale and complexity of its business, the banking sector is expected to maintain robust AML/CFT controls commensurate with its risks. MAS has been applying a rigorous risk-based supervisory approach to banks, comprising on-site and off-site supervision, that is augmented by the use of data analytics. Where weaknesses are observed, findings are shared with the banks as well as 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. Where breaches of laws and regulations administered by MAS are identified, MAS will take the necessary supervisory actions and impose sanctions, proportionate to the severity of the breach.
- 7.3.13 MAS' supervisory activity as well as discussions with banks at ACIP indicate that the banks are aware of their ML risks and have implemented AML/CFT processes and measures to mitigate such risks. This includes the consideration of ML risk indicators as part of customer risk assessment, in the course of performing CDD and for ongoing transaction monitoring and surveillance.
- 7.3.14 Banks in Singapore have been encouraged to use data analytics and advanced detection techniques to identify higher risk customers, including those exhibiting shell company and/or complex structure characteristics, for closer scrutiny. They also apply network analysis to their customers' transactions and counterparties. With network analysis, banks have been able to: (i) uncover hidden relationships, which would have gone undetected had they looked at each customer in isolation; and (ii) improve the quality and timeliness of the STRs filed and provide the LEAs with better leads. Where banks encounter or suspect any property to be connected to criminal activity, they have duly filed STRs. In fact, more than half of the STRs received by STRO were filed by the banking sector.
- 7.3.15 It is important for banks to continue to strengthen their controls, given the volume of funds that pass through their systems (particularly across borders), the broad spectrum of customers they serve (including PEPs and HNWIs) and the range of services and products they offer.
- 7.3.16 To ensure that banks continue to be vigilant in key risk areas and stay alert to emerging threats and vulnerabilities, MAS has performed a series of thematic inspections covering key priority focus areas and ML threats to Singapore including transaction monitoring, foreign tax evasion and corruption risks related to PEPs, PF risks, risks involving the misuse of legal

persons and complex structures and TBML. These thematic inspections have also allowed MAS to benchmark best practices across FIs, identify new emerging typologies and useful case studies. Following these thematic inspections, MAS had shared its key observations and supervisory expectations with the broader industry to enhance their risk awareness and uplift their AML practices.⁵¹

- 7.3.17 The banking industry itself has also taken a pro-active approach to addressing ML/TF risk through ABS. ABS has sought to uplift its members' AML/CFT standards through regular workshops and conferences, engaging MAS on supervisory issues on behalf of its members and clarifying industry best practices.
- 7.3.18 Overall, the banking industry's level of AML/CFT compliance, awareness of ML risks and AML/CFT requirements, and ability to identify and prevent ML are relatively strong. This is particularly true amongst the major banks which make up the bulk of financial sector activity in Singapore, and which are also innovating in the adoption of AML/CFT data analytics to boost their effectiveness and efficiency. However, smaller, less-resourced banks may lag behind their larger counterparts. To this end, MAS and ABS are working closely to uplift their controls through supervisory and industry outreach.
- 7.3.19 Moving forward, MAS continues to explore opportunities to enable greater collaboration amongst FIs to target key ML/TF risks and allow for more effective detection and disruption of major bad actors. MAS recently collaborated with six major banks to establish a digital platform for the exchange of risk information to enhance detection of illicit networks and actors across the sector. This platform is known as COSMIC – Collaborative Sharing of ML/TF Information and Cases.

Box Story 4 – MAS' implementation of COSMIC

To strengthen Singapore's defence against ML/TF/PF risks, MAS has collaborated with six major banks to establish a secure digital platform, named COSMIC (for Collaborative Sharing of ML/TF Information & Cases).

Launched in April 2024, COSMIC allows a participant bank to share customer information with another participant bank if the customer's profile or behaviour displays certain or combinations of indicators of suspicion or "red flags" indicative of potential illicit activities. This will enable the banks to conduct sharper analysis of customer activities. This is aimed at eliminating information gaps that criminals may exploit to conduct illicit transactions through a network of entities with accounts in different FIs, and to enhance detection of illicit networks and actors across the sector.

For a start, information sharing on COSMIC will be among six major commercial banks in Singapore, to allow for agile implementation to achieve platform stability and focus on key risks arising from (a) misuse of legal persons, (b) misuse of trade finance for illicit purposes, and (c) proliferation financing. Information from COSMIC, including material networks of suspicious actors, will be

⁵¹ For example, MAS issued the following papers and guidance: "Guidance for Effective AML/CFT Monitoring Controls" (2018), "Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons" (2019), "Effective AML/CFT Controls in Private Banking" (2020), "Strengthening AML/CFT Name Screening Practices" (2022), "Effective use of data analytics to detect and mitigate ML/TF risks from misuse of legal persons" (2023), and "Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures" (2023).

integrated into MAS' overall surveillance framework to target higher risk activities in the financial system for supervisory intervention as well as WOG mitigation measures.

- 7.3.20 The Covid-19 pandemic has also heightened ML/TF risks in the banking sector. The pandemic resulted in disruptions to banks' normal operating environment and work practices and changed the financial behaviour of customers (e.g. increased demand for remote financial service delivery, changed transactional behaviour/patterns due to the impact of COVID-19 on customers' businesses etc.), which could reduce the effectiveness of some of the FIs' existing profile-based monitoring systems.
- 7.3.21 To support FIs in addressing the operational AML/CFT challenges arising from COVID-19, MAS had provided supervisory guidance to the industry during the onset of the COVID-19 pandemic, on the application of the RBA outlined in our AML/CFT Notices and Guidelines. MAS, together with CAD, had also issued an advisory to alert FIs to emerging COVID-19 related typologies observed internationally and from our ongoing risk surveillance efforts. These have helped FIs cope better with the challenges associated with the pandemic, and in maintaining vigilance towards emerging risks and typologies. The supervisory engagements that followed have shown that key AML/CFT controls in the banking sector have generally continued to operate well, with no major AML/CFT issues noted. Some FIs had adopted alternative solutions, including the use of digital means such as video conferencing, to engage customers. They have also started to explore the use of identity authentication tools to assess if an electronically submitted identification document was genuine. To benefit the broader industry, MAS worked with ACIP to issue a note sharing industry practices which support the effective management of ML/TF risks amidst the pandemic.
- 7.3.22 Overall, in consideration of the banking sector's exposure to high ML threats and given its ML vulnerabilities, it is assessed to pose high ML risk to Singapore, despite the strength of the controls in place for the sector. MAS will continue to subject the sector to enhanced supervisory scrutiny, in line with its RBA. MAS will also continue to leverage FI risk metrics, technology, and analytical tools to conduct risk surveillance of the sector, to proactively identify higher risk banks and activities for follow up action. To help uplift and strengthen the banking sector's AML/CFT controls, MAS will continue to identify and share best practices identified from its supervision with industry, and collaborate closely with ACIP and ABS.

7.4 DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

- 7.4.1 In January 2020, MAS introduced the Payment Services Act 2019 (PS Act), which requires persons that provide DPT⁵² services in Singapore (also known as DPT service providers (DPTSPs))⁵³ to obtain a licence under the PS Act and comply with AML/CFT requirements.

⁵² DPTs, together with digital capital market product tokens, refer to virtual assets as defined in the FATF standards. Entities that conduct regulated activities in relation to digital capital market product tokens are already required to be licensed under the Securities and Futures Act, and to comply with AML/CFT requirements.

⁵³ Virtual assets services providers, as defined in the FATF standards, include DPTSPs.

Key exposures to ML threat areas

- 7.4.2 Globally, it has been observed that cyber-enabled fraud, theft of DPTs, ransomware and transactions in darknet markets⁵⁴ are the main sources of illicit revenue involving DPTs from 2017 to 2022. Research also indicated potential TF/PF risks in relation to the industry. Based on Singapore's risk surveillance, similar threats are observed.
- 7.4.3 Data from LEAs showed an increase in reported cases in Singapore involving DPTs. The majority of the cases involved fraud (e.g. transfer of fraudulent proceeds) or were cybersecurity related offences under the CMA. These largely involved investment scams, which featured online articles using false information to promote DPT investments. Such schemes were found to operate from outside Singapore. Where ML involving DPTs were observed, they were found to be used as a means to transfer proceeds of crime and were largely moved to DPT exchanges based in and outside Singapore. LEAs in Singapore have also observed instances where ransoms demanded featured DPTs. Further, typologies from foreign counterparts have demonstrated close links between ransomware and DPTs, where ransomware criminals often demand payment via DPTs.
- 7.4.4 Based on information from LEAs as well as observations from MAS' surveillance, the three broad ways in which DPTs can be exploited in Singapore would be:
- (i) **payment method:** Ransomware where payment in DPTs is demanded or impersonation scams where scammers impersonate foreign government officials to demand a settlement fee in DPTs. In some cases, tainted assets had flowed through DPT exchanges;
 - (ii) **marketed product:** Schemes involving Initial Coin Offerings (ICOs) or e-commerce scams selling DPTs;
 - (iii) **targeted item:** Unauthorised transactions resulting in the theft of DPTs (e.g. hacking of online wallets/addresses, scams where victims reveal wallet details or private keys).

Box Story 5 – Typologies observed involving DPTs

LEAs in Singapore have observed cases that use DPTs to launder illegal proceeds. In tracing these DPTs, LEAs have managed to trace the DPTs to DPT exchanges, based in Singapore and/or overseas, for a selected number of cases. LEAs leverage international cooperation mechanisms to request for information via STRO or LEA channels on the identity of the perpetrators.

Two emerging typologies are described below:

i. **Victims of Cyber-enabled Fraud Turned Mules Laundering Proceeds Using DPTs**

In certain types of fraud cases (e.g. love scams, and officials impersonation scams), the victims may be deceived into receiving tainted proceeds in their bank accounts without knowledge of their illicit origins. Traditionally, the modus operandi was to request the victims to transfer these funds to other 'pass-through' accounts via a remittance service or wire transfer. Lately, we have seen a new typology in several cases where the perpetrators instructed the victims to purchase and transfer bitcoins to the perpetrators instead.

ii. **Accounts with DPTSPs Set Up Using Stolen Identities to Launder Proceeds**

In cheating cases involving compromised bank accounts (e.g. where victims were deceived into revealing their banking login details), scammers were observed to have layered proceeds by creating an account with a DPTSP in the name of the victims without their knowledge.

⁵⁴ Darknet markets are sites on the dark web where people can buy or sell illicit goods and services online anonymously using cryptocurrency. Examples of the illicit goods and services available are drugs, stolen information, child pornography, and software hacking services.

During account opening, a DPTSP may require the account holder to take a photograph of themselves holding on to their identification document (e.g. passport or national identification card). However, scammers hijack this process by first tricking the victims into taking such a photograph under false pretenses. The criminals would thereafter use this photograph to create an account with a DPTSP, unbeknownst to the victim. The scammer would then transfer funds out from the victim's compromised bank account to the DPTSP for the purchase of DPTs. As the scammer has control of the DPTSP account, they would be at liberty to transfer the criminal proceeds to other accounts under their control, and to launder them through even more layers.

In such cases, the DPTSP may not have detected that its accounts were compromised, despite having conducted the required CDD. From the DPTSPs' perspective, it would appear that the victim was purchasing DPTs using funds from their own bank account.

- 7.4.5 There has also been an upward trend in requests for assistance (RFAs) received via MLAs involving DPTs. The DPT-related RFAs pertained mostly to possible ML, fraud/cheating, and/or drug related offences. Overall, the ML threat posed to DPTSPs is moderately high. A case study relating to ML involving DPTs has been set out below.

Case Study 26 - ML involving DPTs

This case involves a male victim, Person V, who had received a call from a fraudster, who was impersonating the bank. The scammer informed Person V that he might be a victim of credit card fraud and that an investigator would be calling him. Person V subsequently received a call from someone impersonating a Police Officer from the Singapore Police Force. The caller alleged that Person V was a suspect of money laundering and to prove his innocence, Person V would have to transfer his monies to a bank account for verification of the "integrity" of the funds. Following the caller's instructions, Person V transferred a sum of S\$ 1 million into a bank account under his name and relinquished control of the bank account to the scammers.

The scammers registered an account with a DPTSP based in Singapore using Person V's particulars. They then used the monies in the bank account to purchase USDT through the DPTSP. A total of 739,236.04 USDT were purchased, through four transactions, and deposited into a wallet address whose owner could not be identified.

- 7.4.6 The number of STRs filed involving DPTs has also increased, indicating better risk understanding and awareness amongst the regulated sectors that deal with DPTs and DPTSPs, or are DPTSPs themselves. The majority of STRs filed by DPTSPs relate to adverse findings such as bitcoin addresses associated with darknet marketplaces and/or mixers, or suspected fraudulent identification documents, as well as transactions related to online gambling websites. There have also been instances when DPTSPs filed STRs after receiving funds recall requests from victims or financial institutions, as a result of suspected wire transfer fraud. The majority of the STRs relating to DPTs did not point to any specific offence, but the STRs with possible offences disclosed largely related to cheating as well as to cybersecurity related offences under the CMA.

Vulnerability Assessment

Sector characteristics

- 7.4.7 Singapore's status as a FinTech hub has made it an attractive place of business for DPTSPs. Since the commencement of the PS Act on 28 January 2020, approximately 240 firms have submitted applications to MAS for a DPTSP license. MAS has adopted a stringent licensing process and are carefully assessing these applications. As at 31 December 2023, there are 19 licensed DPTSPs.
- 7.4.8 MAS has observed that DPTSPs tend to use business models which are inherently complex and cross-border in nature. Given the pseudonymity, speed and cross-border nature of DPT transactions, they are featured in a number of international typologies for ML, and DPTSPs can be said to be more vulnerable to ML.
- 7.4.9 MAS' surveillance suggests that DPT activity in Singapore has increased from a low base in recent years. Overall, it is noted that DPT activity in Singapore forms a small portion of global DPT activity and is not material compared to traditional financial activities in Singapore's financial system⁵⁵. DPTs are also not actively used domestically as a means of payment.

AML/CFT controls within the sector

- 7.4.10 DPTSPs are regulated under the PS Act and are required to comply with MAS Notice PSN02 on the Prevention of Money Laundering and Countering the Financing of Terrorism for holders of payment services licence (DPT service) and its accompanying guidelines. AML/CFT requirements that are aligned with the FATF Standards, have been imposed on DPTSPs that offer DPT services such as to buy and/or sell DPTs in exchange for money or DPTs in Singapore. Given that DPTs pose inherently higher ML/TF risks, MAS imposes CDD obligations on DPTSPs when business relations are established as well as when any transactions (regardless of amount) are undertaken without business relations. Besides AML/CFT requirements to conduct CDD, perform ongoing monitoring, and report STRs to relevant authorities, value transfer requirements, in line with the FATF Standards also apply to DPTSPs⁵⁶. DPTSPs are also required to comply with CDSA requirements.
- 7.4.11 To further align Singapore's regime with the prevailing FATF Standards, amendments to the PS Act were passed in January 2021 to expand the scope of DPT services to include the service of (i) facilitating the transmission of DPTs; (ii) the provision of custodial services for DPTs; and (iii) facilitating the exchange of DPTs where the service provider does not come into possession of the monies or DPTs involved.⁵⁷ The commencement of the Payment Services (Amendment) Act 2021 is accompanied by the amended Payment Services

⁵⁵ Please see <https://www.mas.gov.sg/news/parliamentary-replies/2021/reply-to-parliamentary-question-on-crypto-asset-market>

⁵⁶ As required under paragraph 13 (Value Transfers) of the MAS Notice PS-N02, digital payment token service providers that facilitate the sending of digital payment tokens are required to obtain and hold required and accurate originator information and required beneficiary information on digital payment token transfers, immediately and securely submit the above information to beneficiary digital payment token service providers and counterparts (if any), and make the information available on request to appropriate authorities. This is aligned with what is known as the "Travel Rule" under the FATF Standards.

⁵⁷ The activity of "participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset", as per the definition of a virtual asset service provider in the Glossary of the FATF Recommendations, would be considered as either a regulated activity under the Securities and Futures Act 2001 or a type of financial advisory service under the Financial Advisers Act 2001.

Regulations and related MAS Notices⁵⁸, with the amendments taking effect in stages from 4 April 2024.

- 7.4.12 MAS has amended MAS Notice PSN02 to include the newly scoped-in payment services. PSN02 was also amended (i) to require licensees and exempt payment service providers under the PS Act which are incorporated in Singapore to develop and implement group-wide AML/CFT policies, and (ii) to introduce requirements relating to agency arrangements of DPTSPs.
- 7.4.13 Given that DPTSPs recently came within MAS' regulatory ambit, MAS is processing the licence applications submitted by existing operators to ensure that they meet stringent fit and proper requirements (including preventing criminals from controlling DPTSPs), adequate compliance arrangements, and requisite AML/CFT policies and procedures. As part of the licensing process, MAS conducts bilateral engagements with DPTSP applicants on the quality of their AML/CFT controls, and to share supervisory expectations, as relevant.
- 7.4.14 To ensure that newly licensed DPTSPs have robust controls, MAS conducted thematic inspections of such selected entities whose businesses were identified to potentially pose higher risk based on data collected via regulatory submissions, to assess their controls in key areas, including enhanced customer due diligence, product risk assessment and sanctions compliance and mitigation. This allowed MAS to have an early sensing of the common areas of weaknesses within the sector which need further clarification and guidance. MAS' supervisory interventions of the sector are supplemented by offsite surveillance of higher risk areas and entities in the DPT space. Specifically, MAS' surveillance aims to look at DPT transactions and networks to detect unusual behaviours or suspicious transactions. MAS also leverages our surveillance capabilities including use of tools such as web and media scrapping, and external data sources to proactively detect entities that may be operating and providing DPT services illegally without a licence. Several unlicensed DPT service providers have been listed on MAS' Investor Alert List to warn consumers that they are not regulated. Where appropriate, MAS refers such entities to LEAs for investigation of unlicensed activities under the PS Act. For example, on 28 January 2021, an individual was sentenced to four weeks' imprisonment for providing DPT services without a licence under the PS Act. The woman had helped to facilitate the transfer of proceeds of crime in the course of providing the unlicensed payment service.
- 7.4.15 We continue to focus on strengthening the level of ML/TF risk awareness and robustness of AML/CFT controls in the DPT sector on an ongoing basis. Noting the higher inherent ML/TF risks posed by DPTs, MAS has regularly engaged the industry through industry townhalls, outreach sessions and webinars since 2019. MAS issued a guidance paper on "Strengthening AML/CFT Controls of Digital Payment Token Service Providers"⁵⁹ in March 2021 to raise industry awareness and provide additional information to facilitate the sector's implementation of effective controls. MAS also plans to issue further guidance in 2024 to share observations from the thematic inspections and provide additional guidance on key controls areas.
- 7.4.16 With MAS' support, the DPT industry has also driven initiatives to promote best practices for AML/CFT and to raise regulatory compliance standards across the sector. For instance, the

⁵⁸ See press release - <https://www.mas.gov.sg/news/media-releases/2024/mas-expands-scope-of-regulated-payment-services>

⁵⁹ See Guidance - <https://www.mas.gov.sg/regulation/guidance/strengthening-amlcft-controls-of-digital-payment-token-service-providers>

Association of Cryptocurrency Enterprises and Start-Ups, Singapore (ACCESS), has collaborated with ABS on a Code of Practice⁶⁰, which aims to provide guidance and promote best practices in relation to AML/CFT for the sector. ACCESS also launched an initiative to conduct independent evaluations of Travel Rule solution providers against FATF Recommendation 16 and technology/cybersecurity requirements to help their members in complying with the FATF's Travel Rule.

- 7.4.17 DPT activities are constantly evolving, with new business models and product offerings emerging. This sector is assessed to pose medium high ML risks. To better monitor the risks arising from this sector, relevant Singapore agencies have come together to collectively monitor and share key risk concerns involving the sector (including at the RTIG). This will allow us to further strengthen AML/CFT regulation of the DPT sector and to facilitate more timely enforcement actions and mitigation measures.

7.5 PAYMENT INSTITUTIONS - CROSS-BORDER MONEY TRANSFER SERVICES

Key exposures to ML threat areas

- 7.5.1 Cross-border money transfer service is defined as any service of accepting money in Singapore, whether as principal or agent, for the purpose of transmitting, or arranging for the transmission of, the money to any person outside Singapore. It also includes any service of receiving any money from outside Singapore for, or arranging for the receipt of any money from outside Singapore by, any person in Singapore, whether as principal or as agent.
- 7.5.2 Internationally, typologies indicate that the cross-border money transfer services channel has been misused by criminals for ML activities in all three stages of the ML process.⁶¹ LEAs have observed instances where the formal cross-border money transfer services channel had been misused, including by shell or front companies for the movement of illicit funds across borders. This includes companies observed to engage in fictitious business transactions to remit/receive illicit funds or to evade foreign tax. There have also been cases where proceeds derived from predicate offences such as fraud or cheating overseas were transferred to Singapore through cross-border money transfer service providers. Conversely, LEAs have also observed cases where proceeds from domestic predicate offences were laundered overseas via these providers. Hence, the ML threat to the cross-border money transfer services sector is moderately high.

Case Study 27

Multiple foreign and local victims of email spoofing fraud transferred monies amounting to at least S\$500,000 into a corporate bank account held by a Singapore-incorporated company, Jars Technology Pte Ltd ("Jars Technology"), and a bank account held by an individual, Mohd Jamail Khan Banakhani Shafi Khan ("Jamail"). Jamail is the director and shareholder of Jars Technology. Jamail claimed that the monies were used for business transactions and investments and provided agreements as exculpatory evidence to CAD during investigations. However, investigations revealed that the agreements were fictitiously created, and some proceeds have been remitted from Jars Technology via a cross border money transfer service from Singapore to UAE.

⁶⁰ See press release – <https://www.access.org.sg/blogs/press-release/access-rolls-out-code-of-practice-to-facilitate-application-of-payment-service-provider-licence-under-singapore-s-payment-services-act>

⁶¹ Source: FATF Report – Money laundering through money remittance and currency exchange providers (June 2010)

In March 2022, Jamail was convicted to 27 months' imprisonment for money laundering offences, a forgery offence, and offences relating to obstruction of justice.

- 7.5.3 There is a segment of cross-border money transfer services that may operate outside the regulatory ambit. Relevant authorities have worked together to put processes in place to mitigate risks arising from this segment. This includes leveraging intelligence to identify unlicensed cross-border money transfer services as well as holistic upstream efforts to encourage users to utilise licensed remittance solutions through outreach and by providing easier access to licensed players.

Case Study 28 – Unlicensed CBMT

In June 2023, U Sun Tin was sentenced to 6 months' jail and fined S\$100,000 for providing an unlicensed cross border money transfer service. His illegal remittance activities were uncovered by the Police during a joint police operation targeted at combatting illegal remittance activities. He was the registered director of a company, Leo International Trading Pte Ltd that was found to have carried on a remittance business and provided cross border money transfer service to assist individuals with transmitting sums to persons in Myanmar. The unlicensed business collected close to S\$30 million over three years from July 2017 to June 2020.

Vulnerability Assessment

Sector characteristics

- 7.5.4 The size of the cross-border money transfer services sector has remained relatively stable over the years. As at end 2023, there were close to 210 cross-border money transfer service providers in Singapore.
- 7.5.5 Singapore has a sizeable foreign community. The United Nation's International Migrant Stock 2020 shows that the percentage of migrants in Singapore has grown over the past three decades, growing from 24% of the population in 1990 to 43% in 2020. The top six migrant nationalities living and working in Singapore in 2020, were Malaysians (45%), Chinese nationals (17%), Indonesians (6%), Indians (6%), Pakistanis (5%) and Bangladeshis (3%). In Singapore, the cross-border money transfer services sector typically caters to resident customers such as individuals (particularly foreign labourers and expatriate professionals) and small and medium-sized enterprises (SMEs). It is an attractive mode of remitting funds to beneficiaries overseas, for personal and business purposes, given its lower transaction fees and wider reach, especially to regions where financial services are less developed. Businesses and foreigners in Singapore thus often make use of formal cross-border money transfer service channels to send funds to beneficiaries overseas.
- 7.5.6 The cross-border money transfer services sector is highly diverse, with providers ranging from small stores to large multi-national companies and web-based businesses. As seen internationally, the cash intensive nature of cross-border money transfer service transactions, especially in brick-and-mortar businesses which typically lend themselves to walk-in and one-off customers, and the sector's ability to process a large number of transactions quickly and conveniently, inevitably expose the sector to criminal elements seeking to misuse the channel to move illicit funds across borders. Reports suggest that cross-border funds flows are inherently vulnerable to being exploited to introduce illicit

funds into the financial system. Given that cross-border money transfer service transactions are generally small individually but are collectively voluminous, it may be easier for suspicious activity, including the structuring of transactions, to be overlooked.

- 7.5.7 The majority of outward cross-border money transfer transactions are transmitted through the local and international banking sector, with most of the remaining transactions transmitted through cross-border money transfer service providers within and outside Singapore. A very small proportion of outward cross-border money transfers may involve informal networks that may not be adequately regulated in foreign jurisdictions for AML/CFT. This may increase the sector's exposure to ML/TF risks. Where such networks are utilised, MAS requires that the cross-border money transfer service provider adequately assess the ML/TF risks involved, which includes subsuming the agent into the service provider's AML/CFT programme and monitoring them for compliance. Where inward cross-border money transfers are concerned, beneficiaries in Singapore generally receive their funds via direct credits to their bank accounts, with a small proportion of transactions involving cash/cheque collections. Overall, considering the cross-border nature of transactions and exposures to customers from other countries, including higher ML risks jurisdictions, the cross-border money transfer services sector is considered to be more vulnerable to ML.

AML/CFT controls within the sector

- 7.5.8 Cross-border money transfer service providers in Singapore are licensed under the PS Act⁶², and MAS Notice PSN01⁶³ on the Prevention of Money Laundering and Countering the Financing of Terrorism. The Notice sets out the obligations of cross-border money transfer service providers to conduct CDD, maintain records, conduct transaction monitoring and file STRs, amongst other requirements. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.
- 7.5.9 MAS takes an RBA approach to its supervision of licensed cross-border money transfer service providers. MAS has observed improvements in the level of ML/TF risk awareness and in the adequacy of AML/CFT processes and controls across the sector over the past few years. More established players within the sector have also been observed to have deployed advanced data analytics capabilities to monitor transactions and detect ML/TF red flags.
- 7.5.10 Over the years, MAS has stepped up our supervision and engagement of the cross-border money transfer service providers to manage risks and identify areas in which AML/CFT controls needs to be enhanced. While there have been overall improvements seen in the level of AML/CFT controls applied by licensed cross-border money transfer service providers, such advancements may be uneven across the sector and the smaller licensed cross-border money transfer service providers may not have scaled up as much as their peers given the discrepancy in resources and systems at their disposal. Another potential risk area that cross-border money transfer service providers should be mindful of is the use of correspondent FIs and agents. While cross-border money transfer service providers would have subjected

⁶² Including for the services of domestic money transfer and cross-border money transfer. Prior to January 2020, they were licensed under the Money-changing and Remittance Businesses Act, and the relevant AML/CFT requirements were found in MAS Notice 3001.

⁶³ Amendments were made to MAS Notice PSN01, which took effect from 4 April 2024, by excluding wire transfers that flow from a transaction carried out using a charge card, credit card, debit card, prepaid card or electronic wallet for the purchase of goods or services from the requirements set out under paragraph 15 of the Notice.

these agents to their internal AML/CFT checks or choose to deal only with agents which are regulated in their home jurisdiction, there are residual risks that these agents (or their agents) may have further engaged intermediaries down the chain, that could have inadequate AML controls.

- 7.5.11 MAS engages its cross-border money transfer service providers on their AML/CFT obligations regularly and has shared common areas of improvement observed from inspection findings as well as key risks involving the potential misuse of cross-border money transfer service providers with the sector.
- 7.5.12 To encourage greater use of the licensed cross-border money transfer service channel in Singapore, MAS has been working with the industry to improve the accessibility and reach of these services, especially for foreign workers. This has been done through the industry's efforts to enhance its online cross-border money transfer service offering (many with native language support). Such services are more likely to be funded by identifiable sources such as electronic bank transfers instead of cash. Some banks have seen an increase in the number of remittance transactions processed, following the suspension of the use of channels that are not specifically permitted⁶⁴ for transfers to the People's Republic of China since 1 January 2024. The suspension seeks to address risks from a consumer protection perspective and to pre-emptively manage the risks of illicit funds being transferred through the cross-border money transfer service providers. MAS has also approved the setup of automated kiosks offering licensed cross-border money transfer services, allowing users to carry out transactions with convenience and ease.
- 7.5.13 Overall, in consideration of the ML threats faced by the sector, its vulnerabilities as well as the strength of the controls in place within the sector, the sector's ML risk is assessed to be medium high. Moving forward, MAS will continue to apply risk-targeted supervision on the sector, through the application of both on-site and off-site supervision. This will serve to ensure that the sector maintains and improves its compliance with its AML/CFT requirements. MAS will also continue to engage the industry through joint initiatives with CAD or through relevant industry associations to convey supervisory expectations and to share emerging ML/TF risk typologies.

7.6 LICENSED TRUST COMPANIES

Key exposures to ML threat areas

- 7.6.1 In the wealth management space, trusts are typically set up by HNWI for succession planning, estate planning, asset protection and philanthropic purposes. LTCs would typically be engaged by these HNWI to establish and administer their trusts.
- 7.6.2 Globally, trusts and other similar legal arrangements pose ML risks as they may be used by bad actors as vehicles to conceal the origin and BO of illicit assets. It is observed that the abuse of trusts and other legal arrangements is more likely occur through professional intermediaries. It is also generally recognised that while the abuse of legal arrangements is less frequent than the abuse of legal persons, LEAs in Singapore have observed at least one instance of suspected foreign tax evasion occurring through trusts set up and administered

⁶⁴ [PSN11 Notice on Temporary Restrictions in Relation to the Provision of Cross-Border Money Transfer Services to the People's Republic of China \(mas.gov.sg\)](#)

by an LTC. (see Case Study 29). Hence, the ML threat to the trust company sector is moderately high.⁶⁵

Vulnerability Assessment

Sector characteristics

- 7.6.3 Singapore's trust company industry has seen a steady growth in trust assets under management over the years, which is in line with the increased demand for wealth management services seen internationally and within the region. As at end 2023, there were over 65 LTCs operating in Singapore, and regulated by MAS as part of the financial sector.
- 7.6.4 A trust allows a settlor to transfer the legal ownership of assets under the trust to a trustee that would hold, and in most instances manage, the trust assets for the benefit of specified beneficiaries. Some trusts could be more sophisticated and have layers of companies in its ownership/control structure as well as in its downstream asset/investment holding structure. Such layers could create a complex structure which could increase the trust's opacity. Hence, a trust arrangement can potentially be used by criminals to mask the BO and to obscure the link between illicit assets/monies and their origins.
- 7.6.5 In general, the trust company sector is also assessed to be more vulnerable to ML because it deals with:
- (i) Higher risk customers such as PEPs and HNWIs, who may also come from higher ML risk jurisdictions;
 - (ii) Complex trust structures as part of wealth management services for HNWIs; and
 - (iii) Cross-border transactions, as a large proportion of customers and assets under trusteeship and/or administration originate overseas.
- Notwithstanding, LTCs do not carry out physical cash transactions and would typically transact with other regulated FIs such as banks. Therefore, there typically is an additional layer of AML/CFT monitoring and gatekeeping by other regulated FIs.

AML/CFT controls within the sector

- 7.6.6 Any person carrying on any trust business or holding himself out as carrying on any trust business in Singapore, must be licensed as a trust company by MAS under the Trust Companies Act⁶⁶. LTCs are required to comply with AML/CFT requirements stated in MAS Notice TCA-N03 on Prevention of Money Laundering and Countering the Financing of Terrorism and its accompanying guidelines. This includes requirements to conduct CDD, maintain records and report suspicious transactions. They are also required to conduct ECDD when any trust relevant party is higher risk, such as a PEP, and to establish their source of wealth and source of funds via appropriate and reasonable means.
- 7.6.7 LTCs are subject to MAS' on-site and off-site supervision, in line with our RBA. Given the higher ML risks posed by the sector, MAS continues to place greater supervisory focus on LTCs. Amongst our supervisory follow-ups with LTCs in the past years, several for-cause inspections of LTCs were triggered because of concerns highlighted by surveillance inputs. MAS uses a combination of (i) supervisory information; (ii) internal data analytics

⁶⁵ Authorities in Singapore are conducting a more detailed analysis of the ML risks relating to legal arrangements.

⁶⁶ Unless an exemption applies. For example, a person may be exempted from holding a licence under the Trust Companies Act where the trust services are carried out by lawyers or accountants. Please refer to the Trust Companies Act and the Trust Companies (Exemption) Regulations for details.

capabilities; and (iii) a control factor assessment⁶⁷ tool to proactively identify specific LTCs of concern for additional supervisory follow-ups. Based on our supervision of the sector, MAS has observed that there is room for improvement in LTCs' AML/CFT controls and monitoring of higher risk trust relevant parties, particularly in relation to the verification of their SoW and the scrutiny of their transactions.

- 7.6.8 Where breaches of AML/CFT requirements are detected, MAS takes proportionate and dissuasive supervisory action. In more severe cases with significant deficiencies in AML/CFT controls, MAS has imposed financial penalties and published the enforcement action. Board and senior management of LTCs who fell short in their duties have also been taken to task.

Case Study 29 – Examples of financial penalties imposed against LTCs in recent years

MAS imposed financial penalties amounting to S\$2.2 million and published enforcement actions against two LTCs for serious breaches of AML/CFT requirements in 2020 and 2022.

The two LTCs failed to implement appropriate AML/CFT procedures and controls to monitor customers who presented higher ML/TF risks. Specifically, the LTCs failed to conduct enhanced monitoring of higher risk customers and did not establish the settlors' SoW/SoF. In addition, one of the LTCs did not subject its AML/CFT controls to independent audits. As a result, the lapses placed them at risk of being used as a conduit for illicit activities.

As part of our ongoing supervision, MAS would closely monitor these LTCs' remediation efforts to ensure that they are effective to address the weaknesses observed. MAS will also require these LTCs to appoint independent parties to provide added assurance on the adequacy and effectiveness of their remediation measures. To-date, the remediation efforts have been completed.

- 7.6.9 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS also published several guidance papers that are relevant to the LTCs, including the following documents (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; (ii) "Circular on Money Laundering and Terrorism Financing Risks in the Wealth Management Sector" in March 2023; and (iii) "Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures" in August 2023. In addition, MAS regularly engages with the LTC industry through townhall sessions to clarify our supervisory expectations on managing ML/TF risks relevant to the LTC sector.
- 7.6.10 The trust industry associations, the Singapore Trustees Association (STA) and The Society of Trust and Estate Planning, have been active in uplifting AML/CFT standards by setting out relevant industry guidance. For instance, an industry led LTC working group led by STA was established to share ML typologies relating to the trust industry and best practices to mitigate the associated ML risks of complex trust structures⁶⁸.

⁶⁷ The control factor assessment was sent to LTCs to assess the LTCs' AML/CFT risk management controls. It is used by MAS as a tool to raise general risk awareness of our supervisory expectations and identify potential breaches of or potential concerns relating to adherence to our AML/CFT requirements proactively.

⁶⁸ In 2022, MAS worked with the Singapore Trustees' Association to develop an industry best practices paper on managing ML/TF risks associated with complex trust structures. Please see: <https://www.sta.org.sg/industry-best-practice-paper/>

- 7.6.11 Overall, in consideration of the sector's exposure to ML threats, its moderately higher ML vulnerabilities as well as the strength of the controls in place within the sector, the LTC sector is assessed to pose medium high ML risk. Hence, MAS will continue its thematic focus and surveillance on LTCs. Through the use of surveillance and analytical tools, MAS will proactively identify LTCs with potential control deficiencies for swifter follow-up. Common weaknesses and best practices identified from MAS' supervision will continue to be shared through townhalls and guidance papers. This iterative process aims to reinforce the LTCs' risk awareness and risk detection, to guide them to better enhance their AML/CFT controls.

7.7 EXTERNAL ASSET MANAGERS

Key exposures to ML threat areas

- 7.7.1 EAMs are fund managers that typically manage the assets of high net worth customers that are custodised with banks on an advisory or discretionary basis, and/or manage funds that are sold to high net worth customers. EAMs face moderately higher ML threats by virtue of their business model – EAMs typically interface between banks and customers, as they are the primary owner of the relationships with such customers, whom they then refer to banks to open accounts. Research on international typologies suggests that foreign high net worth customers (which could include PEPs) may misuse EAMs for foreign corruption, tax evasion or ML activities.

Vulnerability Assessment

Sector characteristics

- 7.7.2 Singapore has positioned itself as a leading wealth management hub for investors and fund managers to locate their investment activities. A large proportion of assets under management in the private wealth space are serviced by EAMs. Singapore has seen fairly strong growth in the number of EAMs and their corresponding total assets under management, with there being approximately 138 EAMs as at the end of 2023.
- 7.7.3 Monies managed by EAMs are typically held in segregated accounts maintained with private banks. EAMs would be granted a limited power of attorney to operate the bank accounts for the sole purpose of managing their customers' investment portfolio.
- 7.7.4 In general, the sector is more vulnerable to ML as EAMs typically deal with: (i) high net worth customers, which could include higher-risk customers such as PEPs, as well as customers from higher ML risk jurisdictions; (ii) complex structures as part of wealth management services for high net worth customers; and (iii) high value cross-border transactions.
- 7.7.5 Notwithstanding, it has been observed that EAMs do not typically deal in physical cash directly, as the monies would have to be deposited with the banks before the EAMs can manage them. Further, the execution of transactions would typically be performed via banks, which are subject to stringent AML/CFT requirements and supervision. This imposes an additional layer of scrutiny over the customer and the customer's transactions. However, some residual risks may continue to exist, particularly if the transactions are executed by banks with weaker controls (e.g. offshore banks in non-FATF compliant jurisdictions).

AML/CFT controls within the sector

- 7.7.6 EAMs carrying out the regulated activity of fund management have to be either licensed or registered with MAS under the Securities and Futures Act (SFA). AML/CFT obligations for EAMs are set out in MAS Notice SFA04-N02 on the Prevention of Money Laundering and Countering the Financing of Terrorism. These include requirements to conduct CDD, maintain records, conduct transaction monitoring and file STRs. They would also need to conduct ECDD when any customer or BO of the customer is higher risk, such as a PEP, and to establish their SoW and SoF via appropriate and reasonable means. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.
- 7.7.7 EAMs are subject to MAS' on-site and off-site supervision, in line with our RBA. Given the higher ML risks posed by the sector, MAS continues to place greater supervisory focus on EAMs. Amongst our supervisory follow-ups with EAMs in the past years, several for-cause inspections of EAMs were triggered because of concerns highlighted by surveillance inputs. MAS uses a combination of (i) supervisory information; (ii) internal data analytics capabilities; and (iii) a control factor assessment⁶⁹ tool to proactively identify specific EAMs of concern for additional supervisory follow-ups. Based on our supervision of the sector thus far, MAS has noted that there is room for improvement in EAMs' ML/TF risk assessment and independent audit frameworks, to more comprehensively understand their vulnerabilities to ML/TF risks, as well as in their execution of key AML/CFT controls. This includes the performance of ECDD measures and ongoing monitoring of customer accounts to detect suspicious transactions.
- 7.7.8 Where breaches of AML/CFT requirements are detected, MAS takes proportionate and dissuasive supervisory action. In more severe cases with significant deficiencies in AML/CFT controls, MAS has imposed financial penalties and published the enforcement action. Board and senior management of EAMs who fell short in their duties have also been taken to task.
- 7.7.9 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS also published several guidance papers that are relevant to the EAMs – including the following documents (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; (ii) "Effective AML/CFT Controls in Private Banking" in September 2020; (iii) "Strengthening AML/CFT Practices for External Asset Managers" in August 2022; and (iv) "Circular on Money Laundering and Terrorism Financing Risks in the Wealth Management Sector" in March 2023.
- 7.7.10 In addition, MAS has regular engagements with the Association of Independent Asset Managers (AIAM), the professional body for EAMs in Singapore, and has highlighted pertinent AML/CFT issues that the EAMs can improve on, such as tax risk surveillance and the need to focus on the adequate implementation of AML/CFT controls. AIAM has committed to work with MAS to uplift the overall AML/CFT standards of EAMs in Singapore. MAS has also supported AIAM in issuing a set of industry-led AML/CFT frequently asked questions (FAQs) in Q4 2020, which provided greater clarity on key AML/CFT concepts specific to the EAM sector.
- 7.7.11 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of the controls in place within the sector, the sector is assessed to be exposed to a medium high level of ML risk. MAS will continue to conduct risk-targeted supervision on

⁶⁹ The control factor assessment was sent to EAMs to assess the AML/CFT risk management controls of FIs. It is used by MAS as a tool to raise general risk awareness of our supervisory expectations and identify potential breaches of or potential concerns relating to adherence to our AML/CFT requirements proactively.

the sector, and will share its findings, including common weaknesses and best practices with the sector to better guide them in their implementation of AML preventive measures.

7.8 FUND MANAGEMENT COMPANIES

Key exposures to ML threat areas

- 7.8.1 Fund management companies (FMCs) are firms which provide their customers with advisory and/or discretionary fund management services. For the latter, FMCs would also place trades with relevant brokers/banks to implement the investment strategies of the funds that they manage.
- 7.8.2 The fund management sector is exposed to transnational ML and could be used to integrate illicit proceeds into the financial system. Having said that, law enforcement has not observed the misuse of FMCs in Singapore thus far. Hence, the ML threat to the FMC sector is assessed to be moderate.

Vulnerability Assessment

Sector characteristics

- 7.8.3 Singapore has a strong pool of regional and global players offering and managing traditional and alternative investment strategies using Singapore as a gateway to source for and access regional investment opportunities. The size of the sector has been growing steadily in recent years, with there being more than 780 FMCs in Singapore as at end 2023 (excluding external asset managers).
- 7.8.4 A large portion of assets under management by FMCs in Singapore are sourced from investors outside Singapore. Hence, they are exposed to some volume of cross-border transactions, including those relating to higher ML risk jurisdictions. However, these FMCs typically serve accredited or institutional investors, including foreign FIs which are subject to 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 advisers and insurance companies, which are similarly supervised by MAS, and required to comply with AML/CFT requirements. The sector in general has a relatively low exposure to higher risk customers such as PEPs.
- 7.8.5 The activities FMCs carry out would also not typically involve physical cash. Customers would generally transfer funds from existing bank accounts to the funds' account for management by the FMCs. FMCs would also typically place trades with brokers or banks, which are subject to AML/CFT requirements and supervision. This arrangement would impose an additional layer of AML/CFT supervision and requirements over the FMC's customers and their transactions.
- 7.8.6 Overall, considering FMCs' exposures to assets and funds sourced from outside of Singapore and exposures to customers from other countries including higher ML risks jurisdictions, the FMC sector is considered to be moderately vulnerable to ML.

AML/CFT controls within the sector

- 7.8.7 FMCs carrying out the regulated activity of fund management are required to either be licensed or registered with MAS under the SFA. FMCs are expected to comply with the AML/CFT obligations set out in MAS Notice SFA04-N02 on Prevention of Money Laundering

and Countering the Financing of Terrorism. These include requirements to conduct CDD, maintain records, conduct transaction monitoring and file STRs. They would also need to conduct ECDD when any customer or BO of the customer is of higher risk, such as a PEP, and to establish their SoW and SoF via appropriate and reasonable means. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.

- 7.8.8 FMCs are subject to MAS' on-site and off-site supervision based on an RBA. MAS uses a combination of (i) supervisory information and (ii) internal data analytics capabilities to proactively identify specific FMCs of concern for additional supervisory follow-ups. Based on its supervision of the sector thus far, MAS has noted that FMCs could further strengthen their oversight of service providers when AML/CFT control functions are outsourced. They could also improve their ML/TF risk assessment and outsourcing frameworks to more comprehensively understand their vulnerabilities to ML/TF risks and could improve in their conduct of ECDD measures. Where there are AML/CFT breaches, MAS ensures that the breaches are rectified in a timely manner. MAS will also take where necessary supervisory actions and sanctions, proportionate to the severity of the breaches.
- 7.8.9 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS published several guidance papers that are relevant to FMCs – including the following documents (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; (ii) "Strengthening Capital Market Intermediaries' Oversight over AML/CFT Outsourcing Arrangement" in July 2020; and (iii) "Circular on Enhancing Anti-Money Laundering and Countering the Financing of Terrorism Controls in the VCC Sector" in September 2022. In addition, MAS regularly engages with the industry via townhall sessions where key AML/CFT observations relevant to the industry would be shared via sector specific case studies.
- 7.8.10 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of the controls in place within the sector, the FMC sector is assessed to pose a medium low level of ML risk. MAS will continue to conduct risk-targeted supervision on the sector, and will continue to share its findings, including common weaknesses and best practices observed, with the sector, to better guide them in strengthening their implementation of AML preventive measures.

Box Story 6 – Variable Capital Companies (VCC)

The Variable Capital Companies Act (VCC Act) and regime was launched in 2020. The VCC Act provides for the incorporation and operation of a new corporate structure, the VCC, to cater to the needs of investment funds managers to provide greater operational flexibility and cost savings. VCCs can only be used to manage investment funds and will accord fund managers in Singapore the flexibility of paying dividends and redeeming shares, as well as the ability to consolidate certain administrative functions, which they were restricted from carrying out under a company structure.

The VCC allows for the separation in legal personality between the VCC and its members, directors and managers. This may potentially allow a natural person to control decisions related to investments and investors, without disclosure of their personal identity.

To address the risks posed by such entities, MAS imposes AML/CFT obligations on VCCs similar to those imposed on FIs. VCC directors are subject to fit and proper checks at the point of the registration of a VCC and as and when there are changes in directorships (or other changes in circumstances e.g. adverse news). They will also be held responsible for any breach of AML/CFT

requirements by their VCC. As a VCC is primarily an investment vehicle, it is required to appoint a fund manager that is regulated⁷⁰ by MAS to manage its investments, and to delegate the execution of its AML/CFT functions to an FI regulated by MAS for AML/CFT, which may be the same entity as its fund manager. As VCCs are set up and run by fund managers, MAS supervises VCCs as part of its supervision of fund managers.

Given the sizeable growth in its use and to assess the adequacy of the VCCs' compliance with their AML/CFT obligations, MAS had conducted a series of thematic engagements of FMCs⁷¹ that are appointed to manage the VCCs. They were selected through risk indicia data collected from VCCs such as exposure to higher risk jurisdictions or PEPs. The focus of the thematic engagement is to understand the FMCs' conduct of AML/CFT measures in respect of the VCCs, including the performance of measures to risk rate customers and conduct ECDD for higher risk customers.

In September 2022, MAS issued a circular to the industry to share key observations from the thematic engagements of the FMCs and highlight supervisory expectations for effective AML/CFT frameworks and controls that VCCs and the relevant FMCs should note.

As a follow-up, in 2024, MAS conducted a targeted risk surveillance review on VCCs, to assess the ML/TF risk posed by VCCs. We observed that the majority of the permissible fund managers/ EFIs appointed by the VCCs continue to be FMCs. From the review of STRs related to VCCs, we have not observed prevalent ML/TF typologies specific to the use of VCCs. Nonetheless, we have identified potentially higher risk FMCs through this review for supervisory follow-ups.

7.9 PAYMENT INSTITUTIONS - MONEY-CHANGERS

Key exposures to ML threat areas

- 7.9.1 Money-changing is the service of buying or selling foreign currency notes and is licensed under the PS Act. International typologies suggest that criminals use money-changers to convert street cash into higher denomination notes⁷², particularly foreign notes, as a precursor to cash movement or cash smuggling across borders.
- 7.9.2 While money-changers were less commonly found to be complicit in ML activities, they have been observed to be particularly susceptible to the receipt and exchange of forged bank

⁷⁰ Generally, a VCC will have to be managed by a fund manager which is a licensed fund management company (i.e. a holder of a capital markets services licence for fund management under section 86 of the Securities and Futures Act), a registered fund management company (i.e. a corporation exempted from holding a capital markets services licence under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations) or a person exempted under the Section 99(1)(a), (b), (c), or (d) of the Securities and Futures Act from the requirement to hold a capital markets services licence to carry on business in fund management (i.e. a bank licensed under the Banking Act, a merchant bank approved under the Monetary Authority of Singapore Act, a finance company licensed under the Finance Companies Act, or a company or cooperative society licensed under the Insurance Act).

⁷¹ These FMCs were appointed as the EFIs to manage the VCCs and conducting necessary AML/CFT checks and performing the measures as required for the VCCs to comply with the requirements in the [MAS AML/CFT Notice VCC-N01](#).

⁷² On 3 November 2020, MAS announced that it would discontinue the issuance of S\$1,000 notes (the largest banknote currently being issued in Singapore) from 1 January 2021, as a pre-emptive move to mitigate the higher ML/TF risks associated with high denomination notes. MAS had previously announced the cessation of S\$10,000 notes in July 2014.

notes. The cash-intensive nature of money-changing and the anonymity of cash also suggest that they may unknowingly receive, and process proceeds of crime. Hence the sector sees a moderate level of ML threats.

Case Study 30

Person L was an employee of a bank, whose duties involved facilitating the hedging of foreign exchange (“forex”) exposure for customers. In this regard, he was allowed to enter forex trades only after he received instructions from customers and had checked with the bank’s treasury desk for prevailing quotes.

Between 2011 and 2013, Person L executed a scheme to conduct unauthorised forex trades in his clients’ accounts, using the accounts maintained by two sole proprietorships controlled by him as counterparties to these trades. Person L then made additional unauthorised trades in other clients’ accounts to close the forex positions of earlier customers. Through this scheme, Person L accumulated benefits amounting to approximately S\$ 1.2 million (approximately US\$ 0.9 million). About 14% of these proceeds were used for purchase of foreign currencies at three licenced money changers in Singapore. The remaining were used to repay his personal loans and credit lines. Information from STRs filed by FIs supported investigations into Person L.

In 2019, Person L was sentenced to imprisonment of 8 years and 4 months for offences relating to the unauthorised modification of computer material, instigating others to commit cheating by personation, and the laundering of proceeds of criminal conduct.

Vulnerability Assessment

Sector characteristics

- 7.9.3 The increased acceptance of electronic payments globally has been observed to have reduced the demand for brick-and-mortar money-changing services, and the size of the money-changing sector has decreased slightly over the years. More recently, the money-changing sector in Singapore has been affected by travel restrictions imposed as a result of the Covid-19 pandemic. Many money-changers experienced a substantial reduction in business and some had chosen to temporarily cease their regulated money-changing operations during this period to reduce costs. As at the end of 2023, there were approximately 380 entities licensed to carry on money-changing in Singapore.
- 7.9.4 The key ML vulnerability for the sector stems from the large amounts of physical cash handled, as the use of cash accords anonymity regarding its source and ownership. Money-changers also deal primarily with walk-in and one-off customer transactions. Money-changing licensees are observed to have lower numbers of higher risk customers (such as PEPs and HNWI). However, the large number of customers they service, which includes foreigners, and the short time taken to process individual transactions, pose challenges to the identification of suspicious transactions. This is especially so when transactions can be deliberately broken down into multiple transactions of smaller amounts to avoid the thresholds for conducting CDD checks.⁷³ Overall, the sector is assessed to be moderately vulnerable to ML.

⁷³ Money-changers are required to conduct CDD checks where it undertakes any transaction of a value exceeding S\$5,000 (except for a specified money-changing transaction where the money is funded from an identifiable source).

AML/CFT controls within the sector

- 7.9.5 Money-changing is licensed under the PS Act⁷⁴, and MAS Notice PSN01 on the Prevention of Money Laundering and Countering the Financing of Terrorism is applicable to money-changers. The Notice sets out the obligations of money-changers to conduct CDD, maintain records, conduct transaction monitoring and file STRs, amongst other requirements. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.
- 7.9.6 MAS has calibrated its supervisory approach to deter non-adherence with regulatory requirements, using a RBA. MAS has noted that while there have been overall improvements seen in the level of AML controls applied by money-changers, general areas where controls could still be strengthened include those relating to the performance of CDD measures, record keeping as well as ongoing monitoring of customer transactions.
- 7.9.7 To mitigate relevant risks involving the sector, MAS conducts thematic inspections of higher risk money-changers with a focus on their performance of CDD, screening, transaction monitoring and record-keeping. This has served to encourage money-changers to continue to be vigilant in performing their AML/CFT obligations, including in relation to transaction monitoring and STR filing.
- 7.9.8 Overall, in consideration of the ML threats faced by the sector, its vulnerabilities as well as the strength of the controls in place within the sector, the money-changing sector is assessed to pose medium low ML risk. MAS will continue to apply risk-targeted supervision on the sector through the application of both on-site and off-site supervision and will work with relevant agencies and industry associations to convey its supervisory expectations and to share relevant and emerging ML/TF typologies with the sector.

7.10 PAYMENT INSTITUTIONS WITHOUT CROSS-BORDER MONEY TRANSFERS (“DOMESTIC PIS”)

Key exposures to ML threat areas

- 7.10.1 The retail payment landscape has seen rapid developments over the past few years. Technological advances have led to the emergence of new retail payment products that involve the issuance of accounts containing e-money to facilitate domestic payments. E-money accounts are prepaid payment products that can be used for several purposes, such as making payments for goods and services, as well as facilitating person-to-person payments. Such accounts can take different forms such as physical prepaid cards, paper vouchers and payment apps.
- 7.10.2 International typologies suggest that e-money accounts may be misused to move illicit funds within a jurisdiction. This is due to the potential anonymity accorded by physical cards and vouchers at the user identification level. E-money accounts may also be anonymously funded, including through cash deposits or funds transfers from other anonymous e-money accounts. In Singapore however, e-money accounts have not been observed to be attractive to criminals, because of the cap on individual account balances and transaction volumes imposed on such facilities.⁷⁵ LEAs have observed some instances where e-money had been

⁷⁴ Prior to January 2020, they were licensed under the Money-changing and Remittance Businesses Act.

⁷⁵ Under the PS Act, personal payment accounts that contain e-money are subject to limits on account balances and transaction volumes, which are set at S\$20,000 and S\$100,000 respectively.

used for ML purposes in Singapore and they largely involve fraud. Hence, the ML threat to the sector is moderate.

- 7.10.3 LEAs have seen some syndicated techniques of abuse concerning e-money accounts. For example, there have been instances where e-money accounts were funded using compromised credit card information or fraudulently created debit cards. The illicit proceeds in these e-money accounts were eventually drawn down to purchase items, withdrawn in cash or deposited into bank accounts in Singapore. STRO has observed that these e-account money issuers often file STRs related to cheating. For instance, STRs have been filed in relation to unauthorised access to payment accounts, credit card fraud, or fraud against the issuer.

Case Study 31 – Syndicated money laundering through e-credits and gift cards

Between April and June 2017, the Police received several reports from victims who were told to transfer cash to bank accounts as deposits for credit-for-sex scams. CAD's investigations revealed that syndicate members operated from China and cheated the victims through social media platforms.

In June 2017, a joint and simultaneous operation with China's Ministry of Public Security was conducted in China and Singapore to take down the credit-for-sex scam syndicate. Three Singaporeans namely Eric Lin Weishen, Elson Lim Yunjun and Melvin Tan Meng Kiat were arrested. The trio had used the cash deposits received from victims to purchase Alipay credits and iTunes gift cards, and subsequently transferred the credits to a foreign syndicate in China. The total amount of criminal proceeds laundered was at least S\$88,000.

Between 2017 and 2018, Melvin, Eric and Elson were charged and convicted to imprisonment of between 10 and 21 months for money laundering.

Case Study 32

This is a syndicated case where Police investigated into ML offences and offences under the CMA, among others. In 2020, Heirul, the mastermind, was sentenced to 27 months' imprisonment for ML and offences under the CMA. Persons Sinhui and May were sentenced to 24 months' supervised probation and fined S\$5,000 respectively.

Between January and February 2019, the three accused created accounts on mobile app services EZ-Link Reload and Singtel Dash to facilitate a payment service fraud. EZ-link provides stored value card which could be used for payment of merchandise in Singapore and offers a cash refund service as one of its features. Singtel Dash offers virtual prepaid card services. After linking the two app accounts, the perpetrators took advantage of an automatic reload function of EZ-link with Singtel Dash when the former reached minimal balances. Under this arrangement, EZ-link allowed users to transact on the 'topped-up' balance while only settling the debt with Singtel Dash at a later stage. Users of the EZ-link app were also able to 'refund' the remaining balance in their accounts to a specified bank account. Thus, by deliberately maintaining insufficient balance in their Singtel Dash accounts, the perpetrators were able to incur mounting debts with EZ-link, which they had no intention of paying off, whilst receiving 'refunds' into their personal bank accounts from which they withdrew cash from ATMs in Singapore. By virtue of using EZ-link in the manner described, Heirul had committed offences under the Computer Misuse Act.

Under this scheme, Heirul managed to obtain 'refunds' into his bank account amounting to a total of approximately S\$36,000, either directly using his own bank account or with the assistance of other parties involved in the scheme, such as Sinhui and May. Heirul subsequently spent the illicit funds on himself.

Vulnerability Assessment

Sector characteristics

- 7.10.4 Although the e-money account issuer sector has grown over the years, it remains fairly small, particularly when compared against other more traditional financial activities in Singapore. Since the commencement of the PS Act on 28 January 2020, approximately 219 firms have submitted applications to MAS to carry on e-money account issuance services. MAS is in the midst of assessing these applications, and as at the end of 2023, there were approximately 50 licensed e-money account issuers in Singapore. Most of the e-money account issuers provide cross-border money transfer services (please refer to risks assessment relating to Payment Institution with Cross-Border Money Transfer in section 7.5 above), and only a small number are domestic PIs.
- 7.10.5 Reports suggest that e-money account issuers may be vulnerable to the potential anonymity of the BO of payment apps (involving ownership and source of funds flowing into the e-money account). That said, it has been observed that e-money accounts in Singapore are generally used by customers who are resident in Singapore and typically for the payments of goods and services. Inflows into e-money accounts in Singapore also largely involve straightforward domestic bank transfers or credit card payments (whose ownership can be readily identified by LEAs), rather than cash deposits. Overall, MAS has observed that limited risks arise from Singapore-issued e-money products, given their limited circulation and functionalities as well as the limits imposed by MAS on their account balances and transaction volumes.⁷⁶ Given so, the domestic PIs sector is assessed to be moderately vulnerable to ML.

AML/CFT controls within the sector

- 7.10.6 Domestic PIs are regulated under the PS Act. MAS Notice PSN01 and PSN01A on Prevention of Money Laundering and Countering the Financing of Terrorism are applicable to domestic PIs. The Notice sets out the obligations of domestic PIs to conduct CDD, maintain records and report suspicious transactions, amongst other requirements. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.
- 7.10.7 MAS takes an RBA to supervision and has calibrated its supervisory approach to domestic PIs accordingly. Based on its supervision and surveillance of the sector, MAS has not observed key weaknesses in the AML controls undertaken by the sector. Overall, in consideration of the ML threats posed to the sector, its vulnerabilities and the strength of its controls, the sector is assessed to have a medium low level of ML risk. MAS will continue to conduct surveillance for new and emerging domestic e-money account issuance models and will identify any ML/TF risks that may be of concern. MAS will also focus future supervisory actions, including inspections, on any emerging threats identified.

⁷⁶ Under the PS Act, personal payment accounts that contain e-money are subject to limits on account balances and transaction volumes, which are set at S\$20,000 and S\$100,000 respectively.

7.11 CAPITAL MARKET SERVICE PROVIDERS - BROKER-DEALERS AND CORPORATE FINANCE ADVISORY FIRMS

Key exposures to ML threat areas

- 7.11.1 Broker-dealers are entities that deal in activities that include:
- (i) Acquiring, disposing, subscribing or underwriting capital markets products⁷⁷ on behalf of any person;
 - (ii) Inducing any person to acquire, dispose, subscribe or underwrite capital markets products;
 - (iii) Providing financing to another person to buy or subscribe for capital markets products; and/or
 - (iv) Providing custodial services.
- 7.11.2 Corporate finance advisory firms mainly provide advisory services to institutional and accredited investors, related to fund-raising, making offers related to capital market products and corporate takeovers and business restructuring.
- 7.11.3 Research on international typologies suggests that the sector's ease of global reach could be misused by criminals seeking to "wash" the taint off illicit proceeds. From LEAs' observations, illicit proceeds could be converted into capital markets products, such as securities; such cases highlight the potential threat of broker-dealers facilitating ML. As we have only encountered one instance where a broker-dealer/corporate finance advisory firm was found to be involved in ML activities⁷⁸, and as the sector has limited exposure to higher risk customers, the sector is assessed to be exposed to a moderate ML threat.

Case Study 33

Acting on information from foreign counterparts that Singapore had received proceeds of crime derived from tax fraud committed in at least two overseas jurisdictions, CAD commenced domestic investigations and seized assets comprising securities and cash in a private banking account in Singapore.

The proceeds were allegedly layered across multiple foreign bank accounts, and subsequently transferred to a Singapore bank account owned by Person A, a foreigner who is not based in Singapore. Person A then transferred the monies to a bank account owned by a company incorporated in Country B. The company is fully owned by a trust incorporated in Singapore, of which Person A is the beneficial owner.

The monies in the account owned by the trust were then used to purchase securities. Assets amounting to a total of GB£12.9 million and US\$7.9 million were seized by CAD. Subsequently, as the accused and the relevant foreign authorities reached a settlement agreement, part of the seized assets were returned to the foreign tax authorities as part of the agreement.

⁷⁷ Capital markets products include securities, collective investment schemes, futures, over-the-counter derivatives and leveraged foreign exchange contracts.

⁷⁸ On 23 October 2020, AGC, CAD and MAS issued a joint statement on actions they would take against Goldman Sachs (Singapore) Pte for its role in the 1MDB bond offerings.

Vulnerability Assessment

Sector characteristics

- 7.11.4 As at end 2023, there were approximately 189 broker-dealers in Singapore conducting one or more of the regulated activities stated above. The business models of these broker-dealers vary in size and complexity, ranging from small firms acting as introducing brokers⁷⁹ to large corporations with exchange clearing memberships⁸⁰.
- 7.11.5 ML risks generally associated with broker-dealers arise from the layering of illicit funds across borders. The sector is characterised by a larger proportion of retail accounts and higher cross-border transaction volumes, which increase the difficulty of effective monitoring of potential ML activities. Broker-dealers have also been observed to engage in transactions with higher-risk customers such as PEPs for investment purposes, and some of these transactions could involve the use of offshore entities.
- 7.11.6 These ML risks are however largely mitigated by the fact that broker-dealers have limited exposure to customers from higher risk jurisdictions. Moreover, the proportion of the sector's physical cash receipts, relative to the total amount of customers' funds handled by the sector, is insignificant. Hence, the sector is assessed to be less vulnerable to ML.

AML/CFT controls within the sector

- 7.11.7 Any FI carrying on the activities specified above is required to hold a capital markets services licence, unless otherwise exempted⁸¹, under the SFA. Licensed broker-dealers are required to comply with AML/CFT requirements stated in MAS Notice SFA04-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism. These include requirements to conduct CDD, maintain records, conduct transaction monitoring and file STRs. They would also need to conduct ECDD when any customer or BO of the customer is of higher risk, such as a PEP, and to establish their SoW and SoF via appropriate and reasonable means. Further guidelines have also been issued to licensees to elaborate on some of the requirements under the MAS Notice.
- 7.11.8 Licensed broker-dealers are subjected to MAS' on-site and off-site supervision based on an RBA. MAS uses a combination of (i) supervisory information; and (ii) internal data analytics capabilities, to profile and proactively identify specific licensed broker-dealers of concern for additional supervisory follow-ups. This includes for-cause inspections on some licensed broker-dealers because of concerns triggered by surveillance inputs. Based on its supervision and surveillance of the sector, MAS noted that broker-dealers could improve their design of ML/TF risk assessment and implementation of ongoing monitoring frameworks, including their conduct of ECDD measures for higher risk customers and screening processes, and STR filing processes.
- 7.11.9 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS also published several guidance papers that are relevant to licensed broker-dealers, including the

⁷⁹ For the purpose of dealing in securities, an introducing broker refers to a corporation which does not carry customer's 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.

⁸⁰ 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 future contracts.

⁸¹ Section 99 of the SFA.

following documents (i) “Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls” in January 2019; (ii) “Enhancing Robustness of Enterprise-Wide Risk Assessment on Money Laundering and Terrorism Financing” in August 2020; and (iii) “Strengthening AML/CFT Name Screening Practices” in April 2022. In addition, MAS regularly engages with the industry and shares key AML/CFT observations relevant to them via industry-specific case studies.

- 7.11.10 Overall, in consideration of the ML threats seen by the sector, its vulnerabilities, as well as the strength of the controls in place within the sector, the sector is assessed to pose medium low ML risk. MAS will continue its supervisory engagement of broker-dealers and corporate finance advisory firms through its on-site and off-site reviews, industry engagements and the sharing of best practices and common weaknesses.

7.12 MONEYLENDERS

Key exposures to ML threat areas

- 7.12.1 The moneylending industry caters to individuals who need financial relief but can neither obtain credit from banks nor offer valuables as a pledge to pawnbrokers. The vast majority of loans are unsecured, and borrowers are protected by borrowing cost caps. There are also limits on the unsecured loan amounts as follows:

Table 4: Limits on unsecured loan amounts

Borrower's annual income	Singapore Citizens and Permanent Residents	Foreigners residing in Singapore
Less than S\$10,000	S\$3000	S\$500
At least S\$10,000 and less than S\$20,000		S\$3000
At least S\$20,000	Six times of monthly income	Six times of monthly income

- 7.12.2 International typologies suggest that criminals may exploit moneylenders by engaging in the moneylending business and “lending” their own illicit funds. This may involve the use of shell companies controlled by the criminals to distance themselves from the business. This scheme obscures the true nature of the funds and further gives the loan repayments a façade of legitimacy. However, our LEAs have not identified cases or intelligence suggesting that this typology is present in Singapore.
- 7.12.3 We have not observed indications that criminals are targeting the (licensed) moneylending sector for ML purposes, although the cash-intensive nature of the industry raises potential ML concerns, given the anonymity of cash. Hence, the sector’s ML threat is assessed to be moderate.
- 7.12.4 UML (dealt with by the Police), which is frequently perpetrated by foreign crime syndicates, continues to be an area of concern for LEAs. However, its impact is mitigated by communication and close cooperation between the LEAs and IPTO, who is the sector supervisor for licensed moneylenders.

Vulnerability Assessment

Sector characteristics

7.12.5 The number of licensed moneylenders has remained stable in recent years with there being 153 licensed moneylenders issuing loans of approximately S\$1.9 billion as at the end of 2023.

7.12.6 Overall, the sector is assessed to be less vulnerable than other assessed sectors. Loans disbursed by licensed moneylenders are domestic in nature, with the majority of their customers being locals, followed by foreigners working or residing in Singapore. The transactions performed are also straightforward loan issuances to customers as well as the collection of loan repayments from customers. Given the statutory limits on the quantum of loans which may be disbursed, moneylending loans are typically small, involving an average loan value of about S\$5,300.

7.12.7 The sector's key vulnerability resolves around its intensity of cash transactions.

AML/CFT controls within the sector

7.12.8 To address its key threats and vulnerabilities, IPTO imposes stringent fit and proper checks to ensure that persons with recent criminal records, including those involved in UML, are not allowed to be involved in⁸², employed by or engaged by any licensed moneylender.⁸³ This serves to ensure that criminals and their associates are prevented from controlling or engaging in moneylending activities.

7.12.9 AML/CFT requirements are also set out for licensed moneylenders in the Moneylenders (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Rules (PMTFPFR) and are elaborated in the Information Guide on the Prevention of ML and CFT for licensed moneylenders⁸⁴. The PMTFPFR requires licensed moneylenders to perform AML/CFT obligations such as to conduct CDD to identify and verify their customers and their BOs, to adopt ECDD for higher risk customers, to file STRs etc.

7.12.10 IPTO adopts an RBA to supervision of licensed moneylenders and assesses each licensed moneylenders' risk profile to sieve out higher risk entities for inspection. In determining the risk profile, a range of risk factors is taken into consideration. This includes the licensed moneylender's transactional volumes and values of loans, its ongoing conduct, its accessibility to best practices, the presence of potentially adverse ML/TF information associated with the licensed moneylender (including STRs filed against it), the profile of its borrowers and its AML/CFT compliance arrangements.

7.12.11 Based on its assessment of the licensed moneylenders, IPTO subjects higher risk licensed moneylenders to more intensive supervisory scrutiny. IPTO has been focusing its supervision on ensuring that licensed moneylenders comply with AML/CFT requirements, including requirements to conduct CDD, perform proper record-keeping etc. In November 2023, IPTO also conducted a survey on its licensed moneylenders to determine their level of AML/CFT knowledge and to allow more targeted supervisory scrutiny. Through inspections conducted thus far, IPTO has observed that licensed moneylenders are aware of their AML/CFT obligations. During inspections, inadequacies observed from some licensed moneylenders

⁸² Including via management or control.

⁸³ All applications for employment with any licensed moneylender in Singapore are subject to approval from the Registrar of Moneylenders.

⁸⁴ <https://rom.mlaw.gov.sg/files/Info%20Guide%202020%20for%20Moneylenders.pdf>

tend to involve record-keeping, review of their internal policies, procedures and controls, and training for employees. However, licensed moneylenders have generally been observed to be prompt in carrying out their rectifications. IPTO also has the ability to impose administrative sanctions and take criminal enforcement actions against licensed moneylenders for any AML/CFT breach.

7.12.12 IPTO communicates with licensed moneylenders through various channels such as inspections, industry briefings and meetings with the Credit Association of Singapore. In particular, in 2018, IPTO gave licensed moneylenders a briefing on their AML/CFT obligations, and highlighted various relevant concerns such as the importance and relevance of understanding the purpose of a loan, scrutinising customer transactions throughout the course of a business relationship etc. Other relevant AML/CFT guidance and information for licensed moneylenders are also available on IPTO's website.

7.12.13 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls it has in place, the sector is assessed to be of medium low ML risk. IPTO will continue to conduct risk-based inspections on licensed moneylenders and to reach out to them on AML/CFT concerns. IPTO will also continue to require licensed moneylenders to approve loans only after having face-to-face contact with their customers, in order to prevent borrowers from transacting with unlicensed moneylenders and/or criminals who may be perpetuating a scam. To reduce the sector's vulnerability to ML, IPTO will continue to encourage licensed moneylenders to move from cash transactions towards electronic transactions with borrowers, including the receiving of payments.

7.13 NON-BANK CREDIT CARD ISSUERS

Key exposures to ML threat areas

7.13.1 Credit cards are payment cards issued to users (cardholders), to enable the cardholder to pay a merchant for goods and services, based on the cardholder's promise to the card issuer to pay them for the amounts used, plus other agreed charges. The majority of credit cards in Singapore are issued by banks (which are subject to AML/CFT requirements and supervision).

7.13.2 Credit cards may be subject to funds flows that are result of criminal activity. They may also be the subject of fraud, where false or stolen identities are used to create credit cards or where credit card details are stolen for fraudulent purposes. Industry, regulators and LEAs have typically considered credit card issuance as posing lower ML threat as compared with other financial products and services.⁸⁵ LEAs have also observed limited misuse of non-bank credit cards (NBCCs) in Singapore, and the sector is assessed to be exposed to a moderate ML threat.

Vulnerability Assessment

Sector characteristics

7.13.3 As at the end of 2023, there were four NBCC issuers operating in Singapore. Given restrictions on cash payments, cash access and credit balances for the sector, NBCCs are not generally observed to be an effective vehicle for ML. The very nature of credit card products poses structural controls/restrictions at the placement and integration stages of ML (for

⁸⁵ Source: Wolfsberg AML Guidance on Credit/Charge card issuing and merchant acquiring activities (2009).

example limitations on the amount of currency that can be accessed and the ability of card holders to insert cash into the financial system). MAS has also observed that NBCCs are typically used by Singapore residents and specific groups of corporate customers (e.g. relating to the tourism sector) for the payment of goods and services. Hence, the sector generally is less vulnerable to ML.

AML/CFT controls within the sector

- 7.13.4 NBCCs are subject to MAS Notice 626A to Credit Card or Charge Card Licensees on the Prevention of Money Laundering and Countering the Financing of Terrorism and their accompanying guidelines. This includes requirements for NBCC issuers to conduct CDD, maintain records and report suspicious transactions, amongst other requirements. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.
- 7.13.5 Recent inspections suggest that oversight and risk control measures for the sector are generally effective and sufficiently mitigate the ML risk associated with the sector. NBCCs have also generally been observed to have employed application screening and fraud monitoring systems in relation to credit card products and services.
- 7.13.6 Overall, the NBCC sector is assessed to pose lower ML risk, considering the ML threat seen by the sector, its vulnerabilities and the strength of controls in place within the sector. MAS takes an RBA to supervision, which includes its supervisory approach for the NBCC sector. MAS will continue to monitor for any new and emerging ML/TF risks that may be of concern for the sector, and will focus supervisory actions, including future inspection plans, on any emerging threats identified.

7.14 APPROVED TRUSTEES FOR COLLECTIVE INVESTMENT SCHEMES

Key exposures to ML threat areas

- 7.14.1 Entities that intend to act as trustee for collective investment schemes which are authorised under section 286 of the SFA (authorised collective investment schemes⁸⁶) for offer to retail investors and constituted as unit trusts must be approved by the MAS and are known as approved trustees.
- 7.14.2 LEAs have not encountered any instance in which approved trustees have been misused for ML purposes in Singapore. Hence, the ML threat to approved trustees is moderately low.

Vulnerability Assessment

Sector characteristics

- 7.14.3 The trust assets under trusteeship by the approved trustees sector in Singapore has remained fairly stable over the years. As at end 2023, there were 16 approved trustees of authorised collective investment schemes in Singapore.
- 7.14.4 Typically, approved trustees in Singapore are deemed to be less vulnerable to ML due to (i) the nature of their business – they have a specific business model that involves other

⁸⁶ This includes restricted schemes constituted in Singapore which are in the list of restricted schemes under the Sixth Schedule to the Securities and Futures (Offers of Investments) (Collective Investment Schemes) Regulations (SF(OI)(CIS)R).

regulated FIs such as fund management companies, banks or financial advisors that are subject to fit and proper as well as AML/CFT requirements; and (ii) collective investment schemes are subject to strict transparency and regulatory requirements (for example the requirement to issue a prospectus in compliance with the SFA). Thus, there are additional layers of AML/CFT monitoring and gatekeeping by other MAS-regulated FIs within the schemes.

AML/CFT controls within the sector

- 7.14.5 Under the SFA, trustees of authorised collective investment schemes are required to be an approved trustee. These approved trustees need to comply with AML/CFT requirements stated in MAS Notice SFA13-N01 on Prevention of Money Laundering and Countering the Financing of Terrorism, and the accompanying guidelines. This includes requirements to conduct CDD, maintain records and report suspicious transactions. They are also required to conduct ECDD when any trust relevant party is of higher risk, such as a PEP, and to establish their SoW and SoF via appropriate and reasonable means.
- 7.14.6 Based on its supervision and surveillance of the sector, MAS has not observed key weaknesses in the AML controls undertaken by the sector. As part of MAS' efforts to raise the industry's risk awareness and standards, MAS also published several guidance papers that are relevant to the approved trustees – including the following documents (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; and (ii) "Enhancing Robustness of Enterprise-Wide Risk Assessment on Money Laundering and Terrorism Financing" in August 2020. In addition, MAS regularly engages with the industry via townhall sessions where we would share key AML/CFT observations relevant to the industry via specific case studies.
- 7.14.7 Overall, and in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, it is assessed to pose lower ML risk. MAS will continue to conduct risk-targeted supervision on the sector, and will continue to share its findings, including common weaknesses and best practices, with the sector to better guide them in strengthening the implementation of their AML/CFT controls.

7.15 FINANCE COMPANIES

Key exposures to ML threat areas

- 7.15.1 Finance companies are primarily in the business of providing fixed and savings deposit services, as well as credit facilities to individuals and corporates.
- 7.15.2 Information from our LEAs suggest that finance companies are not commonly featured as being misused for ML purposes. They are assessed to be less attractive to criminals in general, given the more limited spectrum of products and services that they offer. Hence, the sector is considered to be exposed to a moderately lower ML threat.

Vulnerability Assessment

Sector characteristics

- 7.15.3 There are currently three finance companies operating in Singapore, which have combined assets of over S\$17.5 billion as at the end of 2020. Finance companies are assessed to have lower ML vulnerability, as they generally deal in straight-forward transactions. Finance

companies are not allowed to offer deposit accounts that are repayable on demand by cheque, draft or order. Licensing restrictions also prevent them from dealing in foreign currencies, gold or other precious metals, or to acquire foreign currency denominated stocks, shares or debt securities.

- 7.15.4 Although customers of finance companies are observed to be more likely to perform cash transactions than those of banks, their business is largely domestic. Accordingly, the sector's cross-border ML risks are relatively low and the proportion of higher risk customers that they deal with is also observed to be lower than that seen for banks. Overall, they are assessed to be less vulnerable to ML.

AML/CFT controls within the sector

- 7.15.5 Finance companies are licensed under and governed by the Finance Companies Act and are required to comply with MAS Notice 824 on Prevention of Money Laundering and Countering the Financing of Terrorism and their accompanying guidelines.
- 7.15.6 The AML/CFT requirements and controls in place for the sector are similar to that applicable for banks. Based on its supervision and surveillance of the sector, MAS has not observed key weaknesses in the AML controls undertaken by the sector. Finance companies are also members of ABS and are subject to industry outreach and uplift efforts.
- 7.15.7 Overall, in consideration of the ML threat seen by the sector, the sector's vulnerabilities as well as the strength of the controls in place within the sector, the sector is assessed to pose lower ML risk. MAS will continue to conduct risk-targeted supervision on the sector, and will share its findings, including common weaknesses and best practices, with the sector to better guide them in their implementation of AML preventive measures.

7.16 DIRECT LIFE & COMPOSITE INSURERS

Key exposures to ML threat areas

- 7.16.1 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, while composite insurers write both direct life and general business.
- 7.16.2 The sector sees an inherent ML threat in that it could generate proceeds of crime as a target of fraud. International typologies also suggest that ML risks may be presented by certain products such as life insurance products with single premium payments and high cash value upon surrender, or complex products with returns linked to the performance of an underlying financial asset such as insurance wrappers. Insurance monies could also be laundered through the assignment of policies and payments to third parties. That said, the number of cases involving the sector being misused for ML or fraud in Singapore is low. Hence, the sector is assessed to be exposed to moderate ML threat.

Case Study 34

CPIB received information from one of our foreign counterparts that they are investigating Person A who had allegedly favoured and awarded company contracts to Company X in return for kickbacks. It was suspected that Person A had received the corrupt proceeds via his bank accounts

in Singapore and that he had used part of the corrupt proceeds to purchase three different insurance policies. Without waiting for a formal MLA request to be sent, CPIB facilitated our counterpart's investigations by issuing production orders to the relevant banks. CPIB was able to identify the corrupt fund flows and till date has frozen approximately S\$1.5 million worth of assets belonging to Person A and his spouse. This included the insurance policies purchased by Person A, which were seized prior to their maturity dates. The result of the seizures is pending CPIB's foreign counterpart's investigation findings.

Vulnerability Assessment

Sector characteristics

- 7.16.3 As at the end of 2023, there were 24 direct life and composite insurers in Singapore with assets totalling over S\$300 billion. In general, the sector is assessed to have lower ML vulnerability as direct life and composite insurers deal largely with retail customers and sell most of their policies to individuals. Further, premium payments are generally made via electronic transfers. While cash payments are also accepted, they are typically capped at certain amounts.
- 7.16.4 Direct life and composite insurers largely write Singapore onshore risks. As such, the risk of foreign illicit funds flowing directly into the sector is low. The majority of policy holders are also residents, including expatriate professionals working in Singapore. Hence, the sector is assessed to be less vulnerable to ML.

AML/CFT controls within the sector

- 7.16.5 Any person carrying on any insurance business or holding himself out as carrying on any insurance business in Singapore, must be licensed as an insurer by MAS under the Insurance Act. They are also required to comply with AML/CFT requirements stated in MAS Notice 314 on Prevention of Money Laundering and Countering the Financing of Terrorism, and their accompanying guidelines. This includes requirements for direct life and composite insurers to conduct CDD, maintain records and report suspicious transactions. They are also required to conduct ECDD when any customer or BO of a customer is of higher risk, such as a PEP, including to establish their source of wealth and source of funds via appropriate and reasonable means. When conducting transaction monitoring, ML risk indicators that direct life and composite insurers look out for include purchases of large single premium policies, customers who assign policies to third parties after inception and customers who surrender large value policies early and without an appropriate reason.
- 7.16.6 Taking an RBA, direct life and composite insurers are subjected to MAS' on-site and off-site supervision. MAS uses (i) supervisory information; (ii) internal data analytics capabilities; and (iii) a control factor assessment tool; to profile and proactively identify specific direct life and composite insurers of concern for additional supervisory follow-up.
- 7.16.7 Based on its supervision of the sector, MAS has observed that most direct life and composite insurers have put adequate AML/CFT controls in place, which are commensurate with the nature, size and complexity of their business activities. Direct life and composite insurers have also generally been proactive in rectifying lapses and deficiencies identified by MAS in a timely manner. Where AML/CFT breaches are disclosed, MAS will take the necessary supervisory actions and sanctions, proportionate to the severity of the breach.

- 7.16.8 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS has also published several guidance papers that are relevant to direct life and composite insurers – including (i) Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls in January 2019; and (ii) Enhancing Robustness of Enterprise-Wide Risk Assessment on Money Laundering and Terrorism Financing in August 2020. In addition, MAS regularly engages with the industry via townhall sessions, where key AML/CFT observations would be shared with the industry via relevant case studies.
- 7.16.9 Overall, in consideration of the sector's vulnerabilities as well as the strength of the controls in place within the sector, it is assessed to pose lower ML risk. Nevertheless, MAS will continue to conduct risk-targeted supervision on the sector, and will continue to share its findings, including common weaknesses and best practices with the sector to better guide them in strengthening the implementation of their AML/CFT controls.

7.17 SECURITIES DEPOSITORY

Key exposures to ML threat areas

- 7.17.1 Any person who wishes to engage in trading activities in a securities market operated by the Singapore Exchange will need to open a depository account with the Central Depository (CDP) and a trading account with a broker-dealer. CDP is operated by and acts as a bare trustee for all securities deposited with the CDP. While LEAs have not encountered any instance in which the CDP had been misused for ML purposes in Singapore, international typologies have noted laundering of funds and assets through the securities market. Hence, the ML threat to the CDP is moderate.

Vulnerability Assessment

Sector characteristics

- 7.17.2 Given the size of the sector, and its role in custodising all securities traded on the Singapore Exchange, the CDP is exposed to very limited ML vulnerabilities, as it does not directly engage in trading with customers. Such trades are conducted through other FIs such as broker-dealers and banks, which are also regulated by the MAS for AML/CFT purposes. All persons with CDP accounts are clearly identified and verified by CDP during onboarding. CDP also does not engage in direct funds transactions with customers involving their trades as these are handled by the banks.

AML/CFT controls within the sector

- 7.17.3 CDP is subject to AML/CFT requirements under MAS Notice SFA 03AA-N01 to the Depository on the Prevention of Money Laundering and Countering the Financing of Terrorism. This imposes AML/CFT requirements on the CDP and includes requirements to perform CDD, keep proper records and to file STRs.
- 7.17.4 Based on its supervision and surveillance of the sector, MAS has not observed critical weaknesses in the AML controls undertaken by the sector. Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, it is assessed to pose lower ML risk. MAS will continue to subject CDP to both on-site inspections and off-site supervision to ensure its compliance with its AML/CFT requirements.

7.18 FINANCIAL ADVISERS

Key exposures to ML threat areas

- 7.18.1 Entities conducting one or more of the following regulated activities are required to hold a Financial Advisers' license, unless an exemption⁸⁷ applies:
- (i) Advising others concerning any investment product, other than advising on corporate finance;
 - (ii) Advising others by issuing or promulgating research analysis or research reports concerning any investment product;
 - (iii) Arranging any contract of insurance in respect of life policies.
- 7.18.2 We are not aware of the sector being misused for ML, as it primarily deals with the provision of advice. Financial advisers do not typically handle customer funds nor undertake investment decisions on behalf of their customers in the normal course of their business. Hence, the sector is exposed to moderately lower ML threat. While LEAs have not seen the sector being misused for ML, there have been financial advisers who abused their clients' trust by cheating them to purchase investment and/or insurance products under false representations.

Vulnerability Assessment

Sector characteristics

- 7.18.3 Financial advisers provide financial advisory services relating to capital market products and life insurance policies. Among other things, this entails a financial adviser understanding the financial needs of its customer and providing advice on suitable products that can address those needs. The sector has seen steady growth in terms of revenue over the years, and as at end 2023, there were over 60 licensed financial advisers in Singapore.
- 7.18.4 In general, the sector is less vulnerable to ML as financial advisers largely deal with retail investors, with the sector having limited exposure to higher risk customers such as PEPs. That said, the large number of accounts managed by financial advisers, which includes accounts held by foreign customers who could be from higher ML risk jurisdictions, could potentially increase the difficulties for financial advisers in monitoring customer transactions for possible ML activities. While financial advisers do not typically handle customers' funds or undertake investment decisions on behalf of their customers, they play an important role as gatekeepers as they often act as the first line of defence through their interface with their customers.

AML/CFT controls within the sector

- 7.18.5 Any entity acting as a financial adviser in Singapore in respect of any financial advisory service must be licensed by MAS under the Financial Advisers Act, unless an exemption applies. MAS Notice FAA-06 on Prevention of Money Laundering and Countering the Financing of Terrorism sets out the obligations for financial advisers to mitigate the risk of the financial advisory sector from being misused for ML/TF activities. This includes requirements for financial advisers to conduct CDD, maintain records and report suspicious transactions. They are also required to conduct ECDD when any customer or BO of a customer is of a higher risk, such as a PEP, including to establish their source of wealth and

⁸⁷ 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 under the Insurance Act and holders of capital markets license under the SFA.

source of funds via appropriate and reasonable means. Further guidelines have also been issued to elaborate on some of the requirements under the MAS Notice.

- 7.18.6 Financial advisers are subjected to MAS' on-site and off-site supervision based on an RBA. MAS uses a combination of (i) supervisory information; and (ii) internal data analytics capabilities to profile and proactively identify specific financial advisers of concern for supervisory follow-ups. Based on its supervision and surveillance of the sector, MAS has not observed key weaknesses in the AML controls among financial advisers.
- 7.18.7 As part of MAS' efforts to raise the industry's risk awareness and standards, MAS published several guidance papers that are relevant to financial advisers including the following documents (i) "Guidance to Capital Markets Intermediaries on Enhancing AML/CFT Frameworks and Controls" in January 2019; and (ii) "Enhancing Robustness of Enterprise-Wide Risk Assessment on Money Laundering and Terrorism Financing" in August 2020. In addition, MAS regularly engages with the industry via dialogue sessions where we would share key AML/CFT observations and address queries from the industry.
- 7.18.8 Overall, and in consideration of the ML threats seen by the sector, its vulnerabilities as well as the strength of controls in place within the sector, financial advisers are assessed to pose lower ML risk. MAS will continue its supervisory engagement of financial advisers through both on-site and off-site reviews, industry engagements and the sharing of best practices and common weaknesses observed in the sector.

8. SECTORAL RISK ASSESSMENTS – DNFBP SECTOR

8.1 OVERVIEW

- 8.1.1 This Section sets out the ML risk assessment outcomes of relevant DNFBP sectors in Singapore. International typologies, media reports (e.g. Paradise Papers, Panama Papers, Russian Laundromat etc.) and cases in Singapore have shown that DNFBP sectors are also at risk of being misused for ML, as well as for TF and PF. It is therefore important that the DNFBP sectors are aware of their risks and have robust AML/CFT controls in place to mitigate them. Singapore's AML/CFT regime is only as strong as its weakest link. Hence, every sector and entity in Singapore must play its part in ensuring that it is not misused for illicit purposes.
- 8.1.2 Authorities in Singapore have observed a wide variety of laundering techniques being perpetrated in Singapore. This includes complex and syndicated ML involving the use of structures such as shell and front companies, and which could span across multiple jurisdictions and sectors (including through DNFBPs). Through these structures, illicit proceeds could be channelled into and through Singapore under the guise of legitimate business transactions. They could also be used to perpetrate crime, such as fraud.
- 8.1.3 Taking into account the (i) extent of exposure to the ML threats, including Singapore's exposures to known regional and international ML typologies, as well as other information derived from investigations, intelligence obtained from foreign counterparts, STRs, MLAs, RFAs, (ii) vulnerability of the entities to ML, and (iii) strength of AML/CFT controls of the entities in the DNFBP sector, the assessed ML risks of these entities are summarised in the table below. The detailed ML risk assessments of these entities are set out in the following sections.

Medium High ML risk	Corporate Services Providers (CSPs) Real Estate Agents/Developers Casinos Precious Stones and Precious Metals Dealers
Medium Low ML risk	Lawyers Accountants
Lower ML risk	Pawnbrokers

- 8.1.4 The CSP sector has been assessed to pose a higher level of ML risks than the real estate, casino, and precious stones and precious metals dealers sectors. CSPs have been observed in certain instances to be utilised by foreign criminal elements to aid in the incorporation of shell and front companies, including the procurement of nominee directors. Illicit funds entering Singapore have also been observed to be used by criminals to fund their lifestyle/expenses or be further converted or layered to make their illicit origins more difficult to trace. Such illicit funds have been observed to be held in cash, placed with or used in casinos, or converted into other high value assets such as private real estate and PSPMs, which provide a good store of value (and in some cases offer growth/investment prospects). In some instances, other professional intermediaries such as LTCs⁸⁸, lawyers, real estate agents and accountants have been observed to be involved.

⁸⁸ ML risks assessed under the financial sector.

8.2 CORPORATE SERVICE PROVIDERS

Key exposures to ML threat areas

- 8.2.1 As an international business, financial and trading centre, legal persons such as companies play a pivotal role in supporting commercial and entrepreneurial activities in Singapore. However, LEAs have seen instances of companies being misused for illicit purposes, in both domestic and foreign-origin ML cases involving fraud, corruption, tax evasion, TBML, etc. It has also been observed that a range of companies has typically been misused. In particular, BEC and government officials impersonation scams continue to be key concerns for the Police, and shell companies are increasingly observed to be misused as a means to launder fraudulent proceeds.
- 8.2.2 The Companies Act requires companies to appoint at least one ordinarily resident director. Additionally, foreigners need to engage the services of a CSP to incorporate a company in Singapore. CSPs are business entities and individuals that provide a range of services such as corporate advisory, office hosting, corporate secretarial services, and the filing of statutory returns. As such, foreigners seeking to incorporate a company would typically engage the CSP to procure the services of a nominee director to fulfil the requirement and to incorporate a company as well. While such setups subject CSPs and nominee directors to enhanced regulatory scrutiny, there have been instances of CSPs being misused by foreign criminal elements to incorporate shell companies. Statistics and typologies research by LEAs and STRO indicate that in some instances, foreign criminal elements were able to obscure their identities by utilising the services of CSPs (at times, aided by other professional facilitators) to incorporate shell companies. For instance, it was noted in the Panama and Paradise Paper leaks, that local CSPs (like CSPs in other jurisdictions) were alleged to have created complex structures for their customers, particularly those customers who are based overseas. This will be addressed through the new Corporate Service Providers Bill which will regulate all CSPs with operations in Singapore, regardless of where their clients are based.

Case Study 35 – Conviction of a CSP who had facilitated receipt of criminal proceeds linked to cyber-enabled fraud

CAD undertook ML investigations against Chai Chung Hoong (“Chai”), who was a director and Registered Qualified Individual (RQI) of a CSP, 3E Accounting Pte Ltd. In his personal capacity, he took over as the nominee director of four companies from the CSP who incorporated the companies (the “First CSP”), after he was contacted by an agent purportedly representing the companies. The First CSP had declined to provide further corporate services to the four companies after suspecting that they might be involved in fraudulent activities and had closed the bank accounts which he previously opened for them.

Prior to taking over the companies, Chai did not conduct checks on the foreign directors and shareholders or the companies’ activities. He also did not verify the identity of the agent. After taking over the companies, he did not exercise any supervision over the companies’ activities. On the agent’s request, Chai had also couriered the bank tokens and banking document of the four companies to a foreign address in Lebanon, where none of the foreign directors or shareholders resided. As a result of Chai’s failure to exercise any supervision over the companies, the companies’ banks account received criminal proceeds from BEC, impersonation and love scams of approximately US\$558,404.67 between December 2012 and February 2013.

In March 2022, Chai was convicted of four counts of Section 157(1) of the Companies Act and sentenced to six weeks of imprisonment. He was also disqualified from being a director for five years. As Chai was an RQI, ACRA additionally cancelled his registration in March 2023 as he was not a fit and proper person.

- 8.2.3 ML risks are heightened, when foreign individuals take control of bank accounts, such as those opened by local directors whose services they have procured, to facilitate their transactions without the knowledge of the local directors⁸⁹. Our LEAs have prosecuted professional facilitators who were found to have assisted foreign criminal syndicates in the incorporation of Singapore shell companies and the creation of corporate bank accounts for ML purposes. Please see Case Study 36 below on a professional facilitator who has been convicted for incorporating shell companies and operating bank accounts for a foreign criminal syndicate.

Case Study 36 – Professional facilitator convicted for incorporating shell companies and opening bank accounts in Singapore on behalf of a foreign criminal syndicate to launder criminal proceeds

A Russian, Zkert M. Rushdi (“Rushdi”), a professional intermediary, personally recruited foreigners to become directors of shell companies in Singapore. Thereafter, Rushdi provided these foreign directors with forged documents to open bank accounts in Singapore for these shell companies. A criminal syndicate paid Rushdi between US\$1,500 and US\$5,000 for each company that he successfully incorporated.

Between August 2016 and March 2017, CAD received various complaints from foreign victims based in the US, Australia, Hong Kong etc. These victims had fallen prey to spoofed emails purportedly sent by their business associates and had wired over US\$660,000 into six corporate bank accounts in Singapore. Investigations revealed that Rushdi had facilitated the opening of these bank accounts. CAD further identified 19 other local shell companies related to Rushdi and seized more than US\$1.1 million in 15 bank accounts.

In October 2019, Rushdi was convicted of eight counts of ML charges, for his involvement in an arrangement to facilitate the control of another person’s criminal benefits. He was also convicted of 22 forgery charges, for providing the foreign directors with forged documents to open bank accounts. He was sentenced to a total of 88 months’ imprisonment, and his subsequent appeals against the conviction and sentence were dismissed by the Court.

Vulnerability Assessment

Sector characteristics

- 8.2.4 The CSP sector in Singapore has grown slightly over the years. As at the end of 2023, there were close to 2,800 Registered Filing Agents (RFAs) and 3,500 Registered Qualified Individuals (RQIs)⁹⁰ in Singapore, representing annualised growth of about 1% for the sector since 2016.

⁸⁹ This would involve the opening of corporate bank accounts for these shell companies, where the directors would subsequently send the internet banking credentials and security tokens of these corporate bank accounts abroad to their handlers to facilitate their operation of these bank accounts.

⁹⁰ Registered Filing Agents (RFAs) refers to entities which are registered with ACRA to carry out any transaction with ACRA on behalf of their customers, and RFAs act through individuals who are registered with ACRA as Registered Qualified Individuals. RFAs are required to comply with AML/CFT requirements, and to conduct customer due diligence to ensure that activities are consistent with the customers’ business and risk profile.

- 8.2.5 Corporate entities are set up as distinct legal entities, which include the ability to hold entities and assets in their own name and enter into binding contracts. In Singapore, companies are subjected to provisions under the Companies Act, where the directors of companies may be liable for penalties such as disqualification and debarment for contraventions of the Act. Given the ease of setting up corporate entities⁹¹, it has been observed in certain typologies where shell companies have been set up to put on a cover of legitimacy over criminal activities and obscuring beneficial ownership by distancing the beneficial owner from their assets through the use of complex chains of ownership. CSPs in Singapore provide a range of services which are illustrated in para 8.2.2, which makes the sector vulnerable to ML. These CSPs often receive business leads through referrals from other international professional service providers.
- 8.2.6 Overall, cases involving misuse of legal persons involving CSPs have been observed. On the regulatory front, the existing legislative provisions under the Companies Act and ACRA Act, including the new Corporate Service Providers Bill and Companies and Limited Liability Partnerships (Miscellaneous Amendments) Bill which will be passed in July 2024, will further limit the risks of the CSP sector being misused.

AML/CFT controls within the sector

- 8.2.7 In Singapore, a person needs to have a Singaporean identification document in the form of a National Registration Identity Card or Foreign Identification Number⁹², to transact on ACRA's electronic system for the purposes of setting up a company. Foreigners, who do not have such documents, would have to engage a local CSP for the incorporation of a company in Singapore. In practice, most foreign-owned companies in Singapore⁹³ are incorporated through CSPs, and CSPs are responsible for supporting their customers' corporate compliance obligations through transactions with ACRA.
- 8.2.8 CSPs in Singapore are required to be registered with ACRA as RFAs, which are entities, and act through individuals registered with ACRA as RQIs⁹⁴. All directors, partners, and managers of RFAs must meet minimum fit and proper requirements⁹⁵ before they can be registered and/or have their registration renewed. The RFA cannot be registered if any of its directors, partners or managers have been convicted of offences involving fraud or dishonesty punishable with imprisonment for 3 months or more, if they are undischarged bankrupts, or if they have had their prior RFA registration cancelled in the past two years. Other professional service providers like lawyers and accountants that may assist their customers to set up companies and/or file documents with ACRA, would also have to be registered with ACRA as an RFA and/or an RQI and would be supervised as such. This is in addition to the supervision of their AML/CFT obligations as a lawyer or an accountant by their respective sector supervisor.
- 8.2.9 The Accounting and Corporate Regulatory Authority (Filing Agents and Qualified Individuals) Regulations 2015 set out terms and conditions applicable to RFAs/RQIs. This includes

Lawyers and accountants who assist their customers to set up companies and file documents with ACRA would also have to be registered with ACRA as a RFA and/or RQI and would be supervised as such.

⁹¹ Dissolving a company includes striking off and is subject to objections from relevant regulatory agencies and private creditors, or through winding up procedures.

⁹² See footnote 20 above on Singpass.

⁹³ Regardless of whether they are beneficially owned by Singaporeans, Singapore Permanent Residents or foreigners.

⁹⁴ To be an RQI, an individual must meet criteria prescribed by ACRA.

⁹⁵ Section 31(3) of the ACRA Act.

requirements for RFAs to perform AML/CFT measures such as CDD, which includes identifying and verifying the identities of the BOs of their customers. ECDD requirements are also applicable for higher-risk customers and customers whom they do not meet physically. RFAs are also required to carry out ongoing monitoring of their customers, through which changes to their customers' legal and BO, as well as identity information would be updated. They are also required to file STRs if they come across suspicious activity in the course of their business.

- 8.2.10 Since 2015, ACRA has been issuing guidelines for RFAs to provide clarification on their AML/CFT obligations, which are updated regularly and contain the key AML/CFT risk indicators to assist CSPs in identifying their key threats. In addition, ACRA also publishes periodic guidance papers highlighting the key control weaknesses observed during inspections, for CSPs to note.
- 8.2.11 ACRA has implemented a comprehensive risk-focused supervisory programme to ensure that CSPs fulfil their AML/CFT obligations. When assessing the risk of each CSP, ACRA takes a broad range of risk factors into consideration. These includes the profile of the RFA and its clientele, the type/s of services they provide, their compliance history, referrals from LEAs and other supervisors etc.
- 8.2.12 Since introducing the AML/CFT regime for CSPs in May 2015, ACRA has completed more than 2,900 RFA inspections.⁹⁶ These inspections focus on key ML risk concerns for the sector, such as measures taken to prevent ML/TF, proper identification, verification, and record keeping of legal and BO information, etc. Some common breaches identified include inadequate internal policies, procedures and controls, failure to conduct proper risk assessments as well as failure to screen customers. ACRA conducts additional follow-up inspections on RFAs that are found to be non-compliant with their AML/CFT requirements to ensure that their deficiencies are remediated. In most cases, ACRA observed that the RFAs had rectified the deficiencies, within the period provided by ACRA. In instances where the identified deficiencies were not rectified, ACRA has imposed sanctions, which include penalties⁹⁷ as well as the suspension or cancellation of the registrations of RFAs and RQIs for breaches of ACRA's AML/CFT requirements. There has been an overall increase in AML/CFT compliance levels within inspected CSPs.
- 8.2.13 ACRA also publishes a list of cancelled and suspended RFAs and RQIs on its webpage for public awareness and case facts for egregious cases for industry deterrence. Upon the cancellation of their registration, the RFA or RQI will also be barred from re-registration for a minimum of two years. Any application for registration after that will be subject to closer scrutiny to ensure that the persons satisfy the requisites for registration, including fit and proper requirements. From 2021 to 2023, ACRA cancelled the registrations of 17 RFAs and RQIs. ACRA notes overall that CSPs are generally responsive and cooperative with measures imposed by ACRA to combat ML/TF. There has been an overall increase in AML/CFT compliance levels within inspected CSPs.
- 8.2.14 Within the CSP sector, ACRA has observed CSPs of varying size, ranging from "one-man" operations, which provide limited and less risky transactions such as filing of statutory returns, to larger CSPs which provide a range of corporate services including incorporation, to both local and foreign clients. This difference in the scale of operations has also resulted in varying levels of risk awareness, as well as variances in the adoption of technology to mitigate ML/TF

⁹⁶ As at April 2024.

⁹⁷ Penalties ranging from S\$2,000 to S\$40,000 have been meted out.

risks amongst the CSPs. However, ACRA notes that compliance levels across the industry have increased since the introduction of the AML/CFT regime.

- 8.2.15 To raise CSPs' awareness of their AML/CFT requirements, ACRA introduced mandatory training and proficiency test requirements for CSPs seeking to register or renew as RFAs from November 2018. ACRA has also been working closely with professional bodies such as the Chartered Secretaries Institute of Singapore (CSIS) and The Institute of Singapore Chartered Accountants (ISCA) to uplift professional standards within the sector. ACRA actively participates in various outreach sessions with our professional bodies as well as other engagements. ACRA speaks at the CSP conference organised by the CSIS annually and provides industry updates on a bi-annual basis. At such events, ACRA has taken the opportunity to discuss and share topics such as the role of CSPs during the Covid-19 pandemic, and best practices for the prevention of financial crimes, and invited CAD to share insights on suspicious transaction reports filed by CSPs, etc. ACRA also actively shares AML/CFT publications, including those by FATF, that may be relevant to the CSP sector to strengthen AML/CFT awareness and to encourage the incorporation of best practices within the sector.
- 8.2.16 ACRA subjects CSPs found to have facilitated the misuse of companies, including the setting up of shell companies, to more intensive supervisory scrutiny. While not all CSPs are involved in incorporating shell companies, ACRA has been actively monitoring and striking off inactive companies to address key threats and risks arising from shell companies. Since 2019, ACRA had struck off over 20,000 inactive companies⁹⁸ and disqualified the company directors associated with these companies.

Case Study 37 – Cancellation of RQI Registration

Investigations by the CAD revealed that between July 2020 and February 2021, foreign agents used foreign CSPs (primarily based in China) to engage Singapore CSPs to incorporate local companies and open Singapore bank accounts. In neglecting their duties as directors, the local nominee directors of 35 Singapore-registered companies allowed these foreign agents to operate the company bank accounts. These compromised bank accounts received and laundered criminal proceeds amounting to around US\$36 million originating largely from overseas victims of business email compromise scams.

Among others, the director of one CSP was charged by both CAD and ACRA for breaching director's duties and the lodgement of false information with the Registrar of Companies by authorising her staff to use her Singpass/Corppass account to lodge documents including those relating to the Register of Registrable Controllers, knowing that the documents contained false information that is false in a material respect. In addition, ACRA also took regulatory action to cancel her registration as a RQI and her RFA.

Case Study 38 – Cancellation of CSP Registration and Barring of Re-registration following misuse of companies for cheating offences

An RFA was engaged by Company M to set up 14 local companies and to provide corporate secretarial services. Among other regulatory requirements, the RFA was required by law to conduct due diligence to establish the identities of the BOs of the 14 local companies. ACRA's inspection

⁹⁸ As at 31 Dec 2023.

found that the RFA had failed to do so. Company M had used some of these local companies for cheating offences, which were investigated by the CPIB.

ACRA found that the RFA had committed 29 severe AML/CFT breaches, including failure to inquire on the existence of any beneficial owner and failure to document the details of the risk assessment when performing customer diligence measures, among others. Given the multiple severe AML/CFT breaches, ACRA took decisive action, cancelling the RFA's registration and imposing a two-year ban from acting as an RFA.

8.2.17 To further mitigate the risks posed to Singapore by legal persons, ACRA worked closely with the ACIP Legal Persons and Arrangements working group (ACIP LPA WG) to strengthen the awareness and defences of the financial sector, and support CSPs in raising their risk awareness. In April 2024, the ACIP LPA WG issued a best practice paper on banks' management of the risks associated with receiving referrals from CSPs. Further, the ACIP LPA WG implemented a mechanism for banks to provide ACRA feedback on CSPs that pose ML/TF risk concerns, to facilitate ACRA's targeted supervisory reviews and follow-ups.

8.2.18 To mitigate the risks associated with nominee directors being misused by foreigners when establishing shell companies, ACRA conducts a number of profiling exercises on individuals likely to be nominee directors and sends letters to caution them on compliance risks relevant to their appointment. ACRA also continues to work closely with the LEAs and other sector supervisors to take a WOG approach to tackling concerns arising from shell companies and nominee directors. The Box Story below details ACRA's enforcement actions.

Box Story 7 – Enforcement actions taken by ACRA against nominee directors

In 2019, following a profiling exercise, ACRA took enforcement action against 21 individuals, each found to have held multiple directorships of companies in Singapore. Investigations revealed that these individuals had corporate compliance breaches for failing to hold annual general meetings and to file annual returns for numerous companies under their directorship.

The highest number of charges tendered in court against one of these individuals was 124. Prosecution for all cases have since concluded, and the highest fine imposed by the State Courts was S\$71,400. In addition to receiving fines, all but two of these individuals were disqualified from acting as directors for five years. ACRA has continued with this project of identifying potential nominee directors and subjecting them to greater scrutiny since 2019.

8.2.19 Notably, MOF and ACRA will be passing the Corporate Service Providers Bill and Companies and Limited Liability Partnerships (Miscellaneous Amendments) Bill in July 2024. These two Bills will enhance the regulatory regime for CSPs and the transparency of legal persons. Key changes include expanding the scope of entities that will be regulated as CSPs and increasing the fines for AML/CFT breaches for CSPs, including individuals who own or manage such CSPs. It will also be an offence for individuals to provide nominee directorship services by way of business unless the appointments are arranged by a CSP; CSPs will also be required to be satisfied that these individuals they arrange to act as nominee directors are fit and proper. These amendments will ensure greater accountability from CSPs while also enabling more stringent action to be taken against errant CSPs. Finally, these amendments would also significantly address risks associated with misuse of nominee directorship arrangements.

- 8.2.20 Overall, CSPs are assessed to pose medium high ML risk. To mitigate these risks, ACRA will continue to apply an RBA to sector supervision and take firm and decisive action against errant CSPs. ACRA will also continue engaging the sector to raise their awareness of key and emerging risk concerns, to better guide them in strengthening the implementation of their AML/CFT controls. Additionally, targeted measures have also been implemented over the years, including the upcoming passage of new legislation in the CSP Bill, the setup of a central BO register by ACRA in July 2020, enhanced use of data analytics by ISTR to flag suspicious networks involving shell companies for inter-agency action, thematic supervisory action by MAS on risks involving the misuse of legal persons and complex structures risks seen by FIs etc. Given the cross-cutting nature of the misuse of legal persons, ACRA continues to work closely with the LEAs and other sector supervisors to take a WOG approach to tackling concerns arising from shell companies and nominee directors.

Box Story 8 – ML Risks related to Shell companies and Corporate Services Providers

Since 2017, the misuse of legal persons has been identified as a key risk concern for Singapore. There have thus been various measures undertaken by agencies, including ACRA/MOF, MAS and CAD to address these risks over the years.

Apart from actions at WOG level, public-private partnership is also one of the levers that was used. For instance, the ACIP Legal Persons and Arrangements Work Group (LPA WG), comprising representatives from banks and competent authorities was set up with the aim of strengthening the industry's understanding of risks associated with the misuse of legal persons and arrangements, identifying emerging typologies and risks involving legal persons and arrangements and developing risk products for dissemination. Initiatives undertaken by the LPA WG included the preparation and dissemination of best practices papers on (i) the misuse of legal persons; (ii) wealth management; and (iii) managing ML/TF risks associated with CSPs; and the organisation of a legal persons workshop. Through ACIP's Case Specific Investigation (CSI) mechanism, CAD and other LEAs also worked with the banks on specific cases and trends.

In respect of prosecuting legal persons for ML offences, cases which will advance the public interest and achieve a deterrent outcome will generally be prosecuted. In appropriate cases, both the legal person and the culpable officers will be prosecuted. Fines will be recovered by seizure and sale of the company property if necessary. To achieve a better deterrent effect and create awareness, such prosecutions will be publicised.

8.3 REAL ESTATE AGENCIES, SALESPERSONS AND DEVELOPERS

Key exposures to ML threat areas

- 8.3.1 The real estate sector comprises residential and commercial segments. The residential segment consists of public and private housing, while the commercial segment primarily consists of industrial/office/retail properties. A typical real estate transaction involves parties such as the real estate agency, property developer (for new projects), law practice and FI (where the purchaser requires a loan, or payments are made through the FI for the real estate purchase).
- 8.3.2 The key threat to the real estate sector involves criminals laundering illicit monies through the purchase and sale of properties, which are typically facilitated through real estate agencies

and their salespersons.⁹⁹ International typologies also indicate that criminals are attracted to real estate (e.g. properties) as a channel to launder illicit funds, as the purchase of real estate provides an opportunity to launder a substantial sum in a single transaction. In some cases, real estate also provides a good store of value and has growth/investment prospects. Specifically, international typologies involving the use of real estate for ML have been noted, particularly relating to fraud, foreign corruption or foreign tax evasion.

- 8.3.3 Singapore's economic and political stability have contributed to sound fundamentals in the real estate market and led to the attractiveness of real estate assets in Singapore. This, together with the allowance of visa-free travel for certain nationalities and a large foreign resident presence, increases the risk of the real estate sector being exploited for ML purposes. Criminals are attracted to real estate as a channel to launder illicit funds due to factors such as the high value and safe nature of real estate assets, which can appreciate in value over time. Additionally, the ability to purchase real estate using corporate vehicles or legal arrangements which can disguise the beneficial ownership of a property makes it easier to launder money.
- 8.3.4 Whilst property cooling measures imposed to curtail the increase in property prices, such as Additional Buyer's Stamp Duty for certain buyer segments including foreigners and entities and Seller's Stamp Duty, may reduce the attractiveness of using private residential properties for ML purposes in Singapore,¹⁰⁰ LEAs have observed that real estate assets, remain a means of ML in Singapore, including in the recent major ML case. LEAs noted that there were also cases where the proceeds from domestic organised crimes were converted into real estate assets in Singapore. Illicit proceeds may also be converted into a sizeable number of properties, as shown in the case study below. However, these risks lie predominantly with the private properties market, and Singapore has not observed any cases of misuse of public properties. This is likely due to the unique characteristics of the real estate sector in Singapore, which will be elaborated on further below.

Case Study 39 - Conversion of illicit proceeds into real estate

In 2013, CPIB conducted parallel investigations with one of our foreign counterparts, an LEA from country Y, for ML offences involving Singaporean and Country Y's entities owned by a family (Family X), for giving bribes to a Foreign Public Official from Country Z, in return for advancing the business interest of the entities with Country Z. In July 2016, CPIB charged the Singapore entity for an offence under Section 6(b) of the Prevention of Corruption Act. In June 2018, the Singapore entity was convicted and fined S\$80,000.

⁹⁹ Financial Action Task Force (FATF) (2007), Money laundering and terrorist financing through the real estate sector, June 2007

¹⁰⁰ As of May 2024, foreigners and entities seeking to buy Singapore residential properties are subject to Additional Buyer's Stamp Duty (ABSD) of 60% and 65% respectively, on top of Buyer's Stamp Duty (BSD) (with a marginal rate of up to 6%). These were last increased in Apr 2023 from 30% and 35% for foreigners and entities respectively and are computed based on the purchase price or market value of the property, whichever is higher. Residential property owners who sell their properties within 3 years are additionally required to pay Seller's Stamp Duty of up to 12% (depending on the timing of the sale vis-à-vis the date of purchase). A foreigner looking to purchase a S\$5 million residential property will have to pay BSD/ABSD amounting to around S\$3.24 million. Assuming the property is laundered (sold) within the 1st year at the same price that the property was purchased, the foreigner has to pay an additional Seller's Stamp Duty of S\$600,000. The total amount of tax payable is \$3.84 million, or almost 77% of \$5 million.

Based on the investigation findings of Country Y's LEA, Family X owns 16 properties and five bank accounts in Singapore and there are reasons to believe that the said assets are linked to proceeds of crime. Country Y sent a MACMA request to Singapore to restrain the said assets. Singapore acceded to Country Y's request on 12 March 2020, and 16 properties and two active bank accounts in Singapore were eventually restrained. Four of the 16 properties were registered under the ownership of individuals while the remaining 12 were registered under corporate entities. The two active bank accounts had a combined balance of approximately US\$36.6 million. Investigations by Country Y's LEA on Family X and Country Y's entities owned by the family are on-going.

- 8.3.5 Singapore has also observed professional intermediaries failing to comply with their gatekeeping duties. This includes that of a real estate salesperson. Hence, the ML threat to the real estate sector is moderately high.

Vulnerability Assessment

Sector characteristics

- 8.3.6 As at 1 Jan 2023, there were 1,118 licensed real estate agencies and 34,427 registered salespersons, as well as 213 licensed housing developers in Singapore.
- 8.3.7 In Singapore, public housing constitutes approximately 72% of the total housing stock in 2023, and public housing transactions are tightly controlled by the Government through ownership and occupancy restrictions.¹⁰¹ Foreigners are also not allowed to purchase public housing flats. This makes public housing unattractive and hence less vulnerable to abuse for ML purposes. Further, the authorities have not observed any cases, adverse information or intelligence indicating the misuse of public housing in Singapore for financial crime or ML purposes.
- 8.3.8 Private properties, comprising residential and commercial properties are more freely transacted (except for landed and strata-landed housing properties¹⁰²) and are generally higher in value than the public housing segment. Hence when compared to the tightly controlled public housing segment, the private residential housing segment would be more susceptible to ML.
- 8.3.9 Overall and considering the size of the real estate sector and value of transactions, and some exposure to customers that pose higher ML risks (including foreign customers from higher ML risk jurisdictions), the sector has been assessed to be more vulnerable to ML.

¹⁰¹ For instance, public housing flats sold by the Housing and Development Board (HDB) are meant for Singapore Citizens who meet the eligibility conditions set by the Singapore Government. While Singapore Citizens and Singapore Permanent Residents are allowed to purchase resale HDB flats from the resale market, there is a five-year minimum occupation period before flat owners can sell their flats in the open market. Further, 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.

¹⁰² Strata landed housing properties are residential properties which are not located within an approved condominium development (e.g. townhouse or cluster house). Singapore Land Authority (SLA) requires foreigners to seek prior approval under the Residential Property Act before they can purchase a landed housing, or strata landed housing property in Singapore. SLA assesses each applicant on a case-by-case basis, taking into consideration various factors. Certain conditions must also be met, including that the foreigner must be a Singapore Permanent Resident for at least 5 years and must make exceptional economic contribution to Singapore.

AML/CFT controls within the sector

8.3.10 Within the real estate sector, the gatekeepers are the (a) real estate agencies and salespersons, and (b) developers. They exist as the first line of defence as they come into contact with parties undertaking real estate transactions and therefore play an important role in the prevention and detection of money-laundering activities in property transactions.

Real estate agencies and real estate salespersons

8.3.11 Real estate agencies and their salespersons are regulated under the Estate Agents Act (EAA), which is administered by the Council for Estate Agencies (CEA). Real estate businesses, which include sole-proprietorship, partnerships and companies, are licensed by the CEA and are referred to as real estate agencies. Their salespersons are individuals who perform real estate agency work. Under the EAA, salespersons have to be registered with a real estate agency before they can conduct estate agent work.

8.3.12 CEA ensures that real estate agencies meet relevant fit and proper requirements before they may be licensed to operate. In the circumstances listed below, a person shall not be fit and proper for registration, unless CEA determines otherwise: (a) Where the person has been convicted of an offence involving dishonesty or fraud, or any offence under the EAA; (b) Where the person has had a judgment entered against him/her in civil proceedings that involve a finding of fraud, dishonesty, or breach of fiduciary duties on his/her part; (c) Where the person is an undischarged bankrupt or has made a composition or arrangement with his/her creditors; (d) Where CEA takes the view that a person is not fit and proper after considering any other relevant facts or matters. Additionally, the person is required to declare all prior convictions in a court of law (including a military court), in Singapore or in any other country.

8.3.13 The primary role of real estate agencies and salespersons is to facilitate property transactions for their customers. Where they are involved, the salespersons would typically handle the initial stage of the property transaction, including the marketing of the properties, bringing together buyers and sellers, negotiating prices, and providing advice on policies and procedures relating to property transactions and financing.

8.3.14 The EAA imposes AML/CFT requirements on real estate agencies and salespersons, including CDD, ECDD for higher-risk customers, record keeping and STR filing. This includes requirements for salespersons to identify and verify the BO of any customer that is an entity or a legal arrangement. Real estate agencies are required to ensure that their salespersons undergo training to comply with their AML/CFT duties. Real estate agencies are also required to conduct compliance checks on their salespersons to ensure that the AML/CFT duties are carried out properly.

8.3.15 In addition to legally binding AML/CFT requirements, CEA issues guides to raise the industry's awareness of ML/TF risks in property transactions and provides guidance on the measures real estate agencies and salespersons should take to mitigate the risks of such illicit activities when they facilitate property transactions for their clients. To facilitate the sector's compliance with AML/CFT requirements, CEA has introduced various checklists for real estate agencies and salespersons to assist them to be more effective in implementing their AML/CFT duties and obligations. This includes a checklist for salespersons to facilitate their performance of CDD checks, including the performance of ECDD measures for higher-risk customers, establishing the BO of the transaction and determining the customer/BO's SoF and SoW etc. CEA also issues notices to real estate agencies on AML and targeted financial sanctions

updates, and reminders to comply with AML/CFT duties and file STRs where necessary. CEA also publishes a one-stop AML/CFT resource webpage on CEA's website.

- 8.3.16 CEA adopts an RBA to supervision and subjects higher-risk real estate agencies to more supervisory scrutiny. This includes conducting more regular inspections on higher-risk real estate agencies to assess their compliance with their AML/CFT requirements. CEA also conducts for-cause inspections and carries out investigations whenever it receives any credible adverse information or intelligence on real estate agencies or their salespersons. CEA has conducted 59 inspections on real estate agencies since 2019, including inspections on the five largest real estate agencies which account for more than 80% of the total number of salespersons. Enforcement action, such as reminders, warnings and proceedings before a Disciplinary Committee which led to financial penalties and suspension of registration, has been taken against real estate agencies or salespersons found to be in breach of their AML/CFT obligations.
- 8.3.17 CEA has also engaged in outreach efforts to keep the industry abreast of their AML/CFT obligations and relevant/emerging risks. For example, CEA engages the key executive officers (KEOs) of real estate agencies to discuss key AML/CFT concerns and to reinforce the importance of real estate agencies and salespersons as gatekeepers for the sector. Some of these dialogues are conducted jointly with LEAs and include sharing on the key vulnerabilities and methods of abuse of the real estate sector as well as means to combat such risks through the implementation of appropriate AML/CFT preventive measures. KEOs are encouraged to disseminate key takeaways from these dialogues to their salespersons. More recently in January 2024, CEA conducted an AML/CFT dialogue where representatives from the biggest five real estate agencies in Singapore, real estate agency industry associations, and international property consultants shared and exchanged views on emerging ML risks in the sector and potential mitigation measures.

Developers

- 8.3.18 The development and sale of uncompleted private housing units are regulated under the Housing Developers (Control and Licensing) Act (HDCLA) and administered by the Controller of Housing (COH). The COH also regulates developers in the sale of uncompleted commercial properties, under the Sale of Commercial Properties Act (SCPA). Both the HDCLA and SCPA protect buyers who are buying uncompleted properties "off-plan". To this end, developers of both residential and commercial properties are required to follow standard procedures in the sale of uncompleted units such as the use of standard Options to Purchase (OTP) and Sales and Purchase Agreements (S&PA).
- 8.3.19 For uncompleted private property transactions sold by developers, the purchaser is required to be clearly identified in the S&PA. The purchaser is not allowed to pay for the property purchase in cash, use unidentified nominees to purchase a unit and assign or transfer the OTP to another person.
- 8.3.20 To further enhance the AML/CFT regime for developers, AML/CFT requirements for developers were introduced in June 2023. Under these AML/CFT requirements, fit and proper requirements were imposed to prevent criminals from being involved in developer activities. Housing developers will not qualify for a licence if they have persons holding a responsible position in the developer convicted of an offence involving fraud or dishonesty within 5 years before the date of licence application. To strengthen the detection of ML/TF risks, the HDCLA

was amended to also bar persons from being involved in developer activities if they have been convicted of ML and TF offences.

- 8.3.21 Developers are also required to carry out CDD checks on purchasers, including ECDD for higher-risk customers, ensure proper record keeping relating to these checks and implement adequate programmes and measures to prevent ML/TF activities.
- 8.3.22 The COH has undertaken a series of measures to improve the industry's understanding of risk as well as to ensure that they impose appropriate risk mitigation capabilities to comply with their AML/CFT requirements, for example via guidelines, industry outreach etc.
- 8.3.23 The COH will adopt an RBA to supervision and will focus scrutiny on higher risk developers. Disciplinary action may be taken against any developer found to be in breach of their AML/CFT obligations.
- 8.3.24 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, the real estate sector is assessed to be of medium high ML risk to Singapore. The box story below illustrates the ML risks, and supervisory follow-ups by CEA and URA in the real estate sector in relation to the recent major money laundering case in Singapore. Armed with a better understanding of the overall sectoral ML/TF risk gathered from inspections that CEA has conducted to-date, CEA has refined its risk assessment framework in mid-2023, to allow it to better assess and sieve out higher-risk real estate agencies for more intensive supervisory scrutiny.

Box Story 9 – ML/TF risks in the real estate sector observed in recent major money laundering case

The real estate sector was identified as one of the higher risk sectors and additional efforts were taken to raise industry awareness and tighten our AML/CFT defences.

The key threat to the real estate sector involves criminals laundering illicit monies through the purchase and sale of properties, which are typically facilitated through real estate agencies and their salesperson. A typical real estate transaction involves parties such as the real estate salesperson, property developer (for sale of new property developments), lawyers (whether in processing the sales and purchase or handling the payments) and banks. In this context, the first layer gatekeepers are (a) real estate salespersons, (b) real estate agencies, and (c) developers.

- They are the first line of defence as they are the ones who generally come into first contact with parties undertaking real estate transactions.
- They therefore play an important role in the prevention and detection of money-laundering activities in property transactions.

Enhancements to strengthen the AML/CFT regime in the real estate sector were progressively made over the years. CEA and URA are the regulators who oversee real estate agencies and salespersons, and developers, respectively. To further strengthen the AML/CFT regime in relation to property developers, URA had in June 2023 introduced requirements for developers to perform customer due diligence checks and measures to prevent ML/TF activities.

CEA and URA have undertaken efforts to enhance the awareness of ML/TF risks and the AML/CFT obligations over the years. These efforts include:

- Issuance of a Guide on Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations 2021 by CEA to real estate agencies and salespersons to assist them

in understanding and fulfilling their AML/CFT obligations. The guide contains sample checklists and forms which provides guidance on the conduct of CDD. A similar guide for developers was also issued by COH when the AML/CFT legislations were introduced in June 2023.

- Publication of a list of common suspicious indicators by CEA and URA to aid real estate agencies and salespersons, as well as developers in identifying suspicious transactions, such as when buyers purchase multiple properties in a short time, purchase the properties without inspecting them, or at a value much higher or lower than market value.
- Development of a one-stop resource webpage by CEA, to make it easier for the industry to retrieve information on AML/CFT requirements.
- Conduct of regular briefings to the industry. In this regard, CEA and URA regularly conduct briefings, and have been issuing circulars to guide the real estate sector on the applicable AML/CFT obligations.

Singapore's economic and political stability, as well as its allowance of visa-free travel for certain nationalities and significant foreign resident presence, increase the vulnerabilities of the real estate sector and its risk of being exploited for money laundering purposes. Criminals are attracted to real estate as a channel to launder illicit funds due to factors such as the high value and safer nature of real estate assets, which can appreciate in value over time. Additionally, the ability to finance the purchase of real estate without loans (from banks) or purchase real estate using corporate vehicles or legal arrangements can disguise the beneficial ownership of a property, making it easier to launder money.

The recent S\$3 billion money laundering case has shown how real estate, whether residential or commercial, can be exploited by foreign entities seeking to launder illicit funds. Private residential properties, in particular, have been identified as a prominent channel for money laundering, accounting for approximately 70% of the total number of properties that were issued with prohibition of disposal orders by the Police in the case.

CEA/URA worked closely with Police in that case to identify property transactions by the POIs and properties which were implicated in the case.

- CEA/URA had also issued information notes and circulars to real estate agencies, salesperson and developers to remind them of their AML/CFT obligations, and for the real estate sector to remain vigilant to ML risks.
- Arising from the case, CEA is inspecting and will take appropriate disciplinary actions on real estate agencies and salespersons that are found to have breached the Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations 2021. URA has likewise inspected developers involved in the case to check if they had met AML/CFT obligations applicable at the time of purchase.

8.4 CASINOS

Key exposures to ML threat areas

- 8.4.1 Singapore's integrated resorts – Marina Bay Sands and Resorts World Sentosa - have added a wide array of attractions and amenities to our tourism landscape. There are casinos within both integrated resorts, which are supervised by the Gambling Regulatory Authority (GRA).

- 8.4.2 International typologies indicate that there are inherent ML threats in the casino sector. This takes the form of patrons bringing in and using proceeds of crime in the casinos with the aim of layering and masking the origin of the proceeds of crime and is exacerbated by the cash intensity of the sector, and its ability to allow for the storage and movement of funds, including across borders. However, we have not encountered any instance where the casinos were found to be directly complicit in ML activities in Singapore and have only observed a low number of cases where criminal proceeds were converted to casino chips for self-laundering purposes. Nonetheless, our LEAs have investigated a handful of cases concerning third party ML facilitated by a casino (see case study below). Our FIU has also observed that the majority of STRs filed by casinos do not relate to potential ML offences and instead involve a suspicion of offences under the Casino Control Act or are filed pursuant to adverse news on casino patrons. Overall, the ML threat to casinos is assessed to be moderately high.

Case Study 40 – Conversion of criminal proceeds through gambling activities

While investigating a Singapore bunkering firm that had been conducting short-supply and buy-back transactions of bunker fuel, for conspiracy to cheat vessel owners into paying for extra bunkers that were not delivered, a parallel financial investigation was initiated to pursue possible ML offences.

Investigations revealed that the staff of the bunkering firm would receive commissions from their firm based on their transactions. One of the staff, a programmer, was found to have used most of his proceeds of crime amounting to about S\$1.9 million to purchase casino chips at one of the casinos. After gambling away some of his chips, he encashed his remaining chips including winnings, and used the cash for the payment of his housing and car loans, as well as for the payment of his insurance premiums. On 24 June 2019, the accused was prosecuted for ML involving the conversion of proceeds of crime into casino chips. Court proceedings are ongoing.

Vulnerability Assessment

Sector characteristics

- 8.4.3 The casino sector in Singapore has remained relatively stable over the years, and as at the end of 2023, the total gaming revenue for the sector's two casinos was around S\$5.26 billion. Casinos carry out voluminous transactions of varying amounts on a daily basis, where ML risks may be manifested by way of the mode of transactions or the customer base. A key vulnerability for the casino sector is the cash intensity of its operations. The anonymity of cash 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 become conduits for ML when proceeds of crime transferred to casinos are accepted for the purposes of gambling and are subsequently withdrawn as casino winnings.
- 8.4.4 Both casinos in Singapore attract a large volume of customers, mostly foreign, which may be attributed to their marketing efforts. International Market Agents (IMAs)¹⁰³ may also perform an intermediary role in such efforts to bring in foreign customers, as part of casino marketing arrangements. Any IMA carrying out such functions for casinos in Singapore are subject to a strict licensing regime imposed by GRA. To ensure that criminals do not infiltrate into the casinos, GRA conducts extensive probity checks on IMA applicants to check that they are

¹⁰³ An IMA is an entity licensed by GRA which 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.

suitable to be licensed. Also, if GRA finds a particular licensed IMA to be unsuitable (e.g. involved in criminal acts etc.), GRA has the powers to suspend or cancel their licence. Currently, no IMA is licensed to operate in any of the casinos.

- 8.4.5 Typically, foreign customers' SoW and SoF would originate from overseas. As there is greater challenge and higher complexity in tracing and obtaining information from overseas, this poses a heightened risk in relation to the casinos' ability to verify the legitimacy of the funds. Additionally, the foreign customers may belong to higher ML risk jurisdictions. Such exposure to cross-border transactions increases the sector's vulnerability to ML, and overall, the casino sector is assessed to be more vulnerable to ML.
- 8.4.6 While there are ML risks posed by the casinos, the nature of gaming carries with it a possibility of loss of a significant proportion of criminals' proceeds of crime as gaming outcomes are random and unpredictable. This reduces the attractiveness of casinos being misused as a conduit for ML. Internationally, there are also suggestions that casinos may be less attractive to criminals as compared to other sectors, and where proceeds of crime enter casinos, they largely involve criminals spending the proceeds of crime for leisure, rather than as a means of "washing" criminal funds.

AML/CFT controls within the sector

- 8.4.7 GRA has adopted a strict licensing regime for casino applicants and casino employees, which is supported by the Casino Control Act (CCA). At the point of licence application, GRA will consider whether the casino applicant is of good repute and has undesirable business associations and source of funds. Casino employees performing casino operations are also required to obtain a special employee licence, and probity checks are performed on them. An assessment will also be made of the personal background and financial stability of the applicant, amongst other factors, in determining whether to approve the application.
- 8.4.8 GRA has imposed a comprehensive AML/CFT regime for the casinos via the CCA, the Casino Control Regulations (CCR) and the Internal Controls Code (ICC). Casino operators are required to perform a range of AML/CFT obligations such as CDD, including ECDD for higher-risk customers, and ongoing monitoring of their customers' gaming activities which includes any transactions performed through the casinos.
- 8.4.9 To further mitigate risks arising from its key threats and vulnerabilities, other regulatory requirements that have been imposed on casinos include:
- (i) Casino operators are prohibited from entering into any transaction involving the conversion of money from one form to another when there are insufficient gaming activities to support the conversion. Where patrons request to perform transactions involving the conversion of money from one form to another, the casino operators must check to verify that the patron had wagered at least 90% of his/her original funds before they may proceed with the transaction. In addition, the casino operators are required to have detection mechanisms to flag such suspicious transactions for further assessment and/or reporting. Where there are exceptions noted (e.g. insufficient gaming activities), patrons will have to take out their funds in its original mode, e.g. cash if that was the mode in which the casino first received the funds. For the return of funds via cheques and telegraphic transfer (TT), the casino operators are required to indicate on the cheque or TT transaction that it is for "non-winnings". By the same token, the casino operators can only indicate "casino winnings" for non-cash pay outs if it is verified that the pay outs are casino winnings. To effect this, both casino operators have implemented a three-part document process for cheque payments which comprises the (i) cheque; (ii) customer's

record indicating winnings/non-winnings and details of the cheque which patrons can present together with the cheque to the bank for bank's verification; and (iii) a cheque disbursement form for internal records.

- (ii) Casino operators are prohibited from retaining gaming monies of which the purpose and ownership cannot be ascertained within seven days.
- (iii) Casino operators are also required to file a CTR to STRO for any cash transaction that involves S\$10,000 or more in cash. This applies regardless of whether the cash transaction is performed in a single transaction or across multiple aggregated transactions i.e. the casino operators are required to have measures/procedures in place to track potential structuring activities.

8.4.10 GRA has put in place strong and risk-focused supervisory measures and refreshes its risk assessment of the sector periodically to identify key ML/TF risks and trends for the sector. It inspects both casinos regularly and has focused inspections on various risk themes such as CDD due diligence, STR filing and prohibited transactions.¹⁰⁴ If any weakness or non-compliance with any AML/CFT requirements is observed, GRA ensures that the casino operators take remedial measures as necessary, and within a stipulated timeline. GRA will also investigate and mete out disciplinary actions against the casino operators for failures to comply with their AML/CFT requirements.

8.4.11 GRA has observed that both casino operators have imposed adequate AML/CFT controls and have demonstrated efforts to comply with their AML/CFT requirements. Notwithstanding, there had been instances of AML/CFT related non-compliance identified, and GRA had sanctioned the casino operators accordingly. GRA had also noted that these breaches largely occurred due to human error, resulting in a deviation from adherence to the Standard Operating Procedure in place. To prevent future reoccurrences, the casino operators have committed to imposing more refresher training sessions for their employees.

8.4.12 GRA maintains regular communications with both casino operators to raise and discuss AML/CFT related issues and to keep them informed of pertinent developments relevant to the sector. These include monthly engagements between each casino operator and GRA. The casino operators have been receptive to GRA's suggestions to improve the robustness of their AML/CFT regime, including providing for significant investments into their resources (e.g. IT systems) for better compliance with the AML/CFT requirements.

8.4.13 GRA has also mandated and enforced FATF recommendations and best practices, as adopted from referenced regulators like the US' Financial Crimes Enforcement Network (FinCEN) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) via various AML/CFT regulatory vehicles. Correspondingly, it has observed that the casino operators are generally attuned to the level of ML/TF risks they could be exposed to and have implemented adequate controls to mitigate their ML/TF risks. Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, the sector is assessed to pose medium high ML risk.

8.4.14 To further enhance the casino sector's AML/CFT regime, GRA will be imposing legislative amendments to lower the prescribed CDD threshold for casino transactions, and to align them with the FATF Standards. GRA also reviews existing regulatory requirements periodically, with a view to strengthening the sector's AML/CFT regime. To ensure compliance and effectiveness

¹⁰⁴ Prohibited transactions refer to the transactions set out in 7.3.9(i) and (ii). Additionally, casino operators must not proceed with any transaction which the casino operator has reasonable grounds to suspect that is linked to proceeds of criminal conduct.

of the AML/CFT measures, GRA will continue to perform risk-focused monitoring and inspections of the casino operators commensurate with the moderately higher risks presented by the sector.

8.5 PRECIOUS STONES AND PRECIOUS METALS DEALERS

Key exposures to ML threat areas

- 8.5.1 PSMDs refer to regulated dealers of PSPMs whose activities are defined within the PSPM Act.¹⁰⁵
- 8.5.2 PSMDs are susceptible as conduits to facilitate ML, typically through the placement of illicit funds into PSPMs. International typologies suggest that illicit proceeds, particularly in the form of cash, are typically converted into PSPMs as a store of value (which may appreciate). Domestic law enforcement has come across instances where criminals purchased PSPMs, such as jewellery and gold bars, to convert and conceal the proceeds of crime. The sector is assessed to be exposed to a moderately high ML threat.
- 8.5.3 The following case study features the use of proceeds of crime to purchase PSPMs from PSMDs in Singapore, and the subsequent proceedings brought against the PSMDs involved, including for their failure to file the requisite CTRs.

Case Study 41 – Conviction of PSMDs for their failure to file CTRs

In March 2020, three PSMDs were charged in court for offences under the CDSA.

This was in relation to a series of frauds perpetrated in 2019 by a criminal syndicate against a public agency, which resulted in total losses of S\$40 million. 12 persons have been convicted and sentenced for their involvement in the matter, for a variety of offences, including money laundering. Two of the syndicate members used criminal proceeds to purchase S\$600,000 worth of jewellery and gold bars from the said PSMDs using cash.

In Singapore, PSMDs are obligated to submit a CTR to STRO within 15 business days if they enter into cash transactions exceeding S\$20,000. The three PSMDs were found not to have filed CTRs for the said purchases. Further, one of the PSMDs was found not to have performed CDD, a punishable offence under the CDSA.

Between August and October 2020, the three PSMDs were sentenced to fines ranging from S\$9,000 to S\$40,000.

- 8.5.4 Another case features proceeds of crime derived from predicate offences overseas, that were allegedly used for the purchase of precious metals in Singapore.

¹⁰⁵ Regulated dealing refers to the (a) manufacturing; (b) importing or possessing for sale; (c) selling; (d) purchasing for resale of any precious stone, precious metal or precious product; and (e) selling or redeeming asset-backed tokens.

Case Study 42 - ML involving the purchase of precious metals from a PSMD in Singapore

In 2020, CAD received an MLA request from Country A on an individual, Person B. Person B was indicted in Country A for the promotion of prostitution, sex trafficking as well as ML, and allegedly received more than US\$21 million from these criminal activities. Authorities from Country A had reason to believe that proceeds from Person B's criminal activities were laundered in Singapore.

CAD's ML investigations revealed that Person B had transferred over US\$7.5 million from his overseas bank account to a PSMD in Singapore. Part of these funds were used for trading in precious metals, and the proceeds from such trade were then transferred to a Singapore bank account. During the course of investigations, CAD seized US\$4.5 million from the PSMD and US\$2 million from the bank account. Investigations are ongoing.

Vulnerability Assessment

Sector characteristics

- 8.5.5 The size of the PSMD sector has remained generally stable over the years. As at end 2023, approximately 1,900 PSMDs were registered as regulated dealers in Singapore. The PSMD sector comprises a range of diverse activities and scale of operations, with most PSMDs dealing largely in either the retail or wholesale PSPMs trade.
- 8.5.6 The PSMD sector is more vulnerable to ML risk. PSPMs generally possess high intrinsic value in a relatively compact form that potentially maintains or increases in value over time. PSPMs also facilitate the anonymity of ownership, increasing the sector's vulnerability to ML risk.
- 8.5.7 Certain customer segments of the PSPMs retail sector could present higher ML risk for the sector, as the retail sector deals largely with walk-in and one-off customers. This includes exposure to foreign customers such as tourists, some of whom could be from higher risk jurisdictions.
- 8.5.8 Additionally, large cash transactions present a key risk for PSMDs, given that the use of cash facilitates the anonymity of the transactions and also of the source and ownership of the cash. This could give rise to greater difficulty in establishing the SoW and SoF involved in PSPMs transactions. Payment for PSPMs using DPTs and through bartering gold for jewellery could also pose a higher ML risk, as such payment methods make it difficult to trace the original source and allow the payer to hide their identity.

AML/CFT controls within the sector

- 8.5.9 The Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing Act (PSPM Act) subjects the PSMD sector to a full AML/CFT/CPF regulatory and supervisory regime. The PSPM Act requires regulated dealers to be registered with the Registrar of Regulated Dealers in the AML/CFT Division of the Ministry of Law (ACD), which regulates and supervises the PSMD sector for AML/CFT/CPF purposes.
- 8.5.10 To mitigate the risk of criminals and their associates from controlling or engaging in regulated activities as PSMDs, ACD is empowered to refuse applications for, or renewals of registration to be a regulated dealer. The circumstances for the refusal include instances where the

applicant or its key personnel are found not to be fit and proper.¹⁰⁶ Since 2019, ACD has refused applications for such registration and also cancelled registrations, including over fit and proper concerns. Relevant authorities have also worked together to mitigate the ML risks arising from unregistered dealers. This includes identifying and taking appropriate action against unregistered PSMDs as well as holistic upstream efforts to educate regulated dealers on the requirement to register as a regulated dealer.

- 8.5.11 The legislation is reviewed and amended from time to time, keeping pace with evolving risks. The PSPM Act includes obligations for PSMDs to conduct CDD, ECDD (including establishing source of funds and source of wealth), maintain proper record keeping and perform ongoing monitoring and surveillance of its transactions. PSMDs are also required to file CTRs and STRs in accordance with the law. In November 2023, amendments were made to the subsidiary legislation to the PSPM Act to require PSMDs to conduct CDD measures for transactions involving payment received in DPT above S\$20,000, to address the evolving ML/TF/PF risks inherent in the payment mode.¹⁰⁷ ACD also amended legislation to capture under its regulatory ambit all precious products, as stipulated in the PSPM Act, priced above S\$20,000 regardless of the value attributable to the PSPM, to better address the evolving risk of higher valued precious products which may otherwise not be captured under the PSPM Act.
- 8.5.12 ACD adopts an RBA to supervision, and subjects higher risk PSMDs to more intensive supervisory scrutiny. When assessing the risk of each PSMD, ACD takes a broad range of risk factors into consideration. Supervisory inspections on PSMDs are also triggered by various factors including financial intelligence received or offsite monitoring or surveillance. In line with the sector's key threats and risks, ACD has focused inspections on the performance of CDD, CTR/STR filing, the performance of screening procedures and record keeping. Since the enactment of the PSPM Act in 2019, ACD has conducted over 800 supervisory inspections on PSMDs. Where AML/CFT regulatory offences are disclosed, ACD has taken the necessary supervisory actions and sanctions, proportionate to the severity of the offence. PSMDs are also required to rectify lapses and deficiencies identified by ACD in a timely manner.
- 8.5.13 While there have been overall improvements seen in the level of AML/CFT controls applied by PSMDs, such advancements are uneven across the sector, given the nascency of the regime and the difference in resources and systems at their disposal. ACD therefore continues to conduct briefing and compliance training sessions and issue guidance materials to raise the PSMDs' ML/TF/PF risk awareness, understanding and standards. ACD has also worked closely with the industry associations to co-develop AML/CFT/CPF educational materials and tools for the sector. ACD has provided guidance, including a guidance paper on Strengthening AML/CFT Controls in the Precious Stones and Precious Metals Sector in 2021 to convey supervisory expectations for the PSMD sector. Regular industry engagement sessions have also been conducted to share inspection findings, best practices and supervisory expectations, and emerging ML/TF/PF typologies.¹⁰⁸

¹⁰⁶ The Registrar may refuse to grant or renew registration if the applicant and its substantial shareholder, director, manager, partner, secretary or outlet manager is convicted of money laundering or terrorism financing, an offence involving fraud or dishonesty punishable with imprisonment for a term of 3 months or more, is an undischarged bankrupt, or has a record of non-compliance with requirements for the prevention of money laundering and terrorism financing. The Registrar may also consider any other matters and evidence as may be relevant, that indicated that the applicant poses higher ML/TF risks.

¹⁰⁷ The Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Regulations 2019 (PMLTF Regulations)

¹⁰⁸ Please see <https://acd.mlaw.gov.sg/guidance-materials/>

- 8.5.14 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the general nascency of supervision and controls in place within the sector, the sector is assessed to have medium high ML risk. To further boost the robustness of the sector's AML/CFT/CPF regime, ACD will continue to apply risk-targeted supervision on the sector to ensure that the sector maintains and improves its compliance with its AML/CFT/CPF requirements. It will also continue outreach and training efforts to help PSMDs understand and comply with their AML/CFT/CPF obligations and enhance the sector's ability to better guard against ML risks.

8.6 LAWYERS

Key exposures to ML threat areas

- 8.6.1 Singapore-qualified lawyers may act as both advocates and solicitors. They generally act for and provide legal advice to customers in conveyancing, litigation, corporate advisory (e.g. mergers and acquisition, advisory on new ventures etc.) and other general advisory matters (e.g. wills and estate planning). Registered foreign lawyers in Singapore primarily act as solicitors, although some practise as counsel and offer legal services in relation to international commercial arbitration.
- 8.6.2 Law practices may be abused by criminals seeking to launder illicit proceeds given the services they offer and their veneer of credibility and respectability, which may help distance or structure transactions/funds from their illicit sources. In Singapore, law enforcement has investigated at least one instance where a lawyer was used to facilitate a property purchase involving the proceeds of crime (see Case Study 43). LEAs have also encountered a few instances where lawyers had misappropriated funds held in client accounts, and one case where a lawyer was prosecuted for dishonestly inducing customers to deposit monies into accounts under his control and subsequently laundered them.

Case Study 43 - Failure by professional intermediaries to file an STR

Ezubao was operating as an online peer-to-peer lending finance company in China until the Chinese authorities uncovered a large-scale Ponzi scheme. More than 20 individuals have been convicted of fraud and other offences and sentenced to imprisonment ranging from three years to lifetime imprisonment. Among others, proceeds from the Ezubao Ponzi scheme were intended to be used to purchase a private residential property in Singapore worth more than S\$23 million. Eventually the proceeds were seized, amounting to S\$27 million. These proceeds were successfully returned to China in August 2018.

A real estate agent referred a foreign customer who was interested in purchasing a property in Singapore to a Singapore lawyer for conveyancing. The lawyer subsequently discovered that the foreign customer had been arrested in his home country in relation to the Ezubao Ponzi scheme and was under investigation for fraud. The lawyer and real estate agent suspected that the monies provided by the customer for the purchase of the property were illicit proceeds, but did not file an STR. In 2018, they were convicted of failure to file an STR and fined S\$10,000 each.

- 8.6.3 The cases observed in Singapore are broadly similar to that seen in the international typologies, which indicate that the purchase of real estate provides an opportunity to launder a substantial sum in a single transaction and may be attractive to criminals, also as real estate

may serve as a store of value (and often provides capital gains). It was further observed that the majority of STRs filed by lawyers in Singapore relate to real estate property transactions. International typologies also suggest that client accounts may be used to hold and move monies on behalf of their customers (including for illicit services).¹⁰⁹ The overall ML threat to the legal sector is assessed to be moderate.

Vulnerability Assessment

Sector characteristics

- 8.6.4 The legal sector in Singapore has remained relatively stable over the years. As at end 2023, there were more than 7,400 lawyers and 1,100 law practices registered in Singapore.
- 8.6.5 In Singapore, conveyancing lawyers play a key role in real estate transactions, including holding and processing stake-holding deposits and purchasers' monies for their customers. The use of a legal person or arrangement to hold real estate would further distance the BO from the asset at hand.
- 8.6.6 As noted, client accounts¹¹⁰ and escrow accounts, especially pooled accounts, also present some ML risk. Monies of illicit origin may move through these accounts swiftly and in large sums to third parties. Such accounts may break the audit trail and "cleanse" the funds, as the payments to the third parties would now appear to have emanated from the law practices. Similarly, payments to law practices could easily be represented as payment for legal fees which could sometimes be used to obfuscate its actual purpose or origins. Given this, Singapore-qualified lawyers must account for funds that pass through their client accounts annually.
- 8.6.7 Lawyers may also render trust advisory and management services. Trust arrangements allow a settlor to transfer the legal ownership of assets under the trust for the benefit of specified beneficiaries. Therefore, a trust arrangement can potentially be used by illicit actors to mask BO and create layers that obscure the link between illicit monies and their origins and presents risk for the sector. That said, lawyers involved in the administration of sizeable trust arrangements would generally operate via LTCs, which are also regulated by MAS for AML/CFT in Singapore.
- 8.6.8 More recently, lawyers have been observed to render advisory services on new types of ventures in the emerging technology sector, such as advising on DPT, digital asset licensing, marketing and structuring projects. Law practices in Singapore also provide and/or facilitate legal and tax structuring, company incorporation, professional director services, transactional implementation, escrow services and general advisory services in the technology sector. Such ventures could give rise to new risks, given the generally lower level of understanding of such new products and the more nascent AML/CFT supervisory regime imposed on digital payment token service providers internationally. Therefore, the sector is assessed to be moderately vulnerable to ML.

¹⁰⁹ The risks relating to lawyers being involved in corporate secretarial services (e.g. setting up of companies) have not been included in this NRA as these lawyers are regulated as CSPs in Singapore.

¹¹⁰ According to the Legal Profession (Solicitors' Accounts) Rules, a "client account" means – (a) a current or deposit account maintained in the name of a solicitor at a bank; or (b) deposit account maintained in the name of a solicitor with an approved finance company, in the title of which account the word "client" appears.

AML/CFT controls within the sector

- 8.6.9 Singapore-qualified lawyers are admitted to¹¹¹ the Supreme Court and are regulated on AML/CFT and disciplinary matters by the Law Society of Singapore (Law Society), which works closely with Minlaw. All Singapore-qualified lawyers are required to have a valid practising certificate, which is renewed annually. To renew their practising certificate, Singapore-qualified lawyers are required to satisfy the requirements of the Legal Professions Act 1966¹¹² and, where applicable, show that their accounts are in order.¹¹³ To renew their Certificate of Registration with the Legal Services Regulatory Authority (LSRA)¹¹⁴, foreign-qualified lawyers are required to: (i) declare any past or pending criminal and disciplinary proceedings; and (ii) provide an admission certificate or a certificate of good standing. Where a valid practising certificate is required by their home jurisdiction in order to practise overseas, the foreign-qualified lawyer is also required to submit this document to LSRA.
- 8.6.10 The Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015 and the Law Society's Practice Direction 3.2.1 on the Prevention of Money Laundering and Financing of Terrorism also impose comprehensive AML/CFT requirements on the legal sector, including the obligations to carry out CDD, identify and verify BOs and higher-risk customers, file STRs, and undergo training.
- 8.6.11 In Singapore, it is not necessary to engage lawyers to form companies. Nevertheless, some law practices may offer this service, especially as part of a broader suite of services. However, to do so, the law practice must be licensed by ACRA as a CSP. The risk in relation to CSPs is covered in a separate section. Additionally, when acting for a corporate entity, lawyers are required to identify and verify the identities of the entity's beneficial owners.
- 8.6.12 In accordance with the Conveyancing and Law of Property (Conveyancing) Rules 2011, lawyers in Singapore involved in conveyancing are prohibited from holding conveyancing money on behalf of their customers in their client accounts. Any money received by a lawyer in connection with a conveyancing transaction must be placed in a conveyancing account¹¹⁵ managed by the law practice in accordance with the Conveyancing Rules, or with the Singapore Academy of Law. Lawyers are also obliged to conduct CDD checks, including on their customer's SoF and SoW. Lawyers have an obligation to report receipt of cash originating from outside Singapore if it exceeds a prescribed amount.¹¹⁶
- 8.6.13 Every year, the Law Society inspects about 50 law practices to ensure compliance with their AML/CFT obligations. These inspections are carried out using an RBA. The inspection findings have generally been satisfactory, with only a minority of inspected law practices found to be unsatisfactory. Law practices and/or lawyers found not to be satisfactorily compliant with

¹¹¹ All Singapore-qualified lawyers are registered with the Supreme Court and all foreign-qualified lawyers practising in Singapore are registered with the Legal Services Regulatory Authority.

¹¹² This would include declaration of whether the solicitor: (a) had previously been suspended from practice; (b) had been sentenced to a term of imprisonment; (c) was convicted of an offence: (i) involving dishonesty or fraud; or (ii) in relation to conduct in the practice of law; or (d) had been found guilty of misconduct in any other professional capacity.

¹¹³ See for example sections 25, 25A, 26 and 73 of the Legal Profession Act 1966.

¹¹⁴ The LSRA is a department under the Ministry of Law, helmed by the Director of Legal Services, who oversees the licensing and regulation of all law practice entities and the registration of foreign lawyers, regulated non-practitioners, as well as Singapore solicitors practising in foreign law practices in Singapore.

¹¹⁵ According to the Conveyancing Rules, a "conveyancing account" means a bank account with an appointed bank – (a) maintained, by a solicitor for the purpose of depositing conveyancing money; and (b) in the title of which the word "Conveyancing" or the abbreviation "CVY" appears after the name of the solicitor.

¹¹⁶ Section 62 CDSA

their AML/CFT requirements will be subject to sanctions, ranging from censures/warnings and fines, to being struck off the roll or suspended from practice.

- 8.6.14 The Law Society conducts regular surveys, interviews and targeted seminars to promote awareness of ML/TF risks amongst its members and to understand their risks. For example, the Law Society conducts regular AML seminars and has an AML online learning platform for the sector. It also distributes AML/CFT materials through its website and via correspondence with its members, including a guidance on complying with CDD requirements and trade-based ML risks for law practices.
- 8.6.15 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, the sector is assessed to be of medium low ML risk to Singapore. The Law Society conducted a sector-wide AML/CFT survey in 2021 to gather more data for a deeper understanding of the sector's key risk concerns and the risk assessment framework for the legal sector is regularly reviewed. Further, in view of the recent major ML case, the authorities will continue to monitor and review the ML risks of the legal sector.

8.7 ACCOUNTANTS

Key exposures to ML threat areas

- 8.7.1 In Singapore, professional accountancy services are mainly provided by public accounting entities owned and managed by public accountants. Public accountancy services are defined in the Accountants Act as the audit and reporting of financial statements and other acts that are required to be performed by a public accountant. Public accountants provide public accountancy services to the public through accounting corporations, LLPs, partnerships or sole proprietorships (accounting entities).
- 8.7.2 Apart from public accountants, there is another group of professional accountants, who are not registered as public accountants, as they do not provide any public accountancy services. Most of them are members of the ISCA. Such professional accountants mainly either work with public accountants to provide various accountancy-related services or are in-house accountants employed by companies, businesses or government agencies that provide limited services within the scope defined by the FATF.
- 8.7.3 International typologies suggest that the accounting sector is at risk of exploitation for high-end ML, as accountants can provide a sense of legitimacy to falsified accounts, or as part of their corporate advisory work. In Singapore, LEAs have not observed many ML cases involving the accounting sector. Within the limited cases encountered, there were instances where accountants had misappropriated funds entrusted to them and self-laundered them for their own benefits (see Case Study 44). Hence, the overall ML threat for the sector is assessed to be moderate.

Case Study 44 - Accountant prosecuted in an embezzlement and laundering case developed directly from an STR

In 2017, STRO received an STR on Person A, who was an accountant of a Singapore incorporated company, Company B. STRO's analysis revealed that Person A had deposited multiple cash cheques issued by Company B into his Singapore bank account. Subsequently, the funds were drawn down

via cash withdrawals. The cash cheques issued by Company B were each below S\$10,000 and were sequentially numbered.

Acting on the financial intelligence, CAD initiated an investigation into Person A. Investigations revealed that Person A was authorised to sign singly for Company B's cheques of up to S\$10,000. Between April 2013 and June 2017, Person A misappropriated nearly S\$4 million from Company B by issuing cash cheques to himself and depositing most of them into his bank accounts in Singapore. Thereafter, he withdrew the monies in cash from his bank accounts and remitted approximately S\$3 million to overseas bank accounts in his name or in the name of his family and friends on 835 occasions across 241 days, via various remittance agencies.

In 2019, Person A was sentenced to nine and a half years' imprisonment for offences, which included CBT and transferring the benefits of criminal conduct. CAD seized over S\$22,000 of the proceeds. The rest had either been expensed or transferred out of Singapore. CAD has sent an MLA request to follow up on the proceeds which had been transferred out of Singapore.

Vulnerability Assessment

Sector characteristics

- 8.7.4 The accounting sector has remained relatively stable over the years. As of 31 March 2023, there were over 4,200 professional accountants (i.e. ISCA members) in public practice, of which 1,210 were public accountants practising in 720 accounting entities.
- 8.7.5 Both public and professional accountants may provide a veneer of legitimacy to falsified accounts as they may review and sign off on accounts of customers engaged in illicit activities. The accounts may be used to conceal illicit fund flows or facilitate the laundering of illicit proceeds. Accountants may also facilitate other crimes such as tax evasion, including goods and services tax fraud, or through the provision of corporate advisory services, which may involve the use of complex structures. Such complex structures could also be used to mask beneficial ownership and create layers that obscure the link between illicit monies and their origins and presents risk for the sector. However, as accountants do not typically handle customer monies, their vulnerability to exploitation by criminals seeking to launder criminal proceeds is more limited. Overall, accountants are assessed to be moderately vulnerable to ML.

AML/CFT controls within the sector

Public accountants and accounting entities

- 8.7.6 Public accountants are persons registered with and regulated by ACRA for the purpose of performing public accountancy services and are subject to the requirements in the Accountants Act and the rules and standards prescribed pursuant to the Accountants Act.
- 8.7.7 In all new applications for the registration of public accountants, the applicant must meet prescribed requirements relating to qualifications, practical experience, continuing professional education and registration as a Chartered Accountant (Singapore). Consideration is also given to whether the applicant has been convicted of a criminal offence, whether the applicant has been subject to any investigation for an offence involving dishonesty, whether the applicant is an undischarged bankrupt and whether there are any adverse records against the applicant, etc. If found to be not fit and proper, ACRA will reject the public accountant application. Similarly, accounting entities are put through checks, which consider various

criteria including whether its partners and directors are subject to adverse records. ACRA also regularly screens existing public accountants and accounting entities against third-party screening software and any adverse records may result in disciplinary action being taken against them. Thus far, there have been no instances where ACRA detected an individual who was not fit and proper while performing ongoing monitoring.

- 8.7.8 Public accountants and accounting entities are required to comply with the AML/CFT requirements set out in the Accountants (Prevention of Money Laundering and Financing of Terrorism) Rules 2023. ACRA adopts an RBA to its supervision of public accountants and accounting entities and focuses its inspections on higher-risk accounting entities. To determine the ML/TF risk of each accounting entity, ACRA takes a range of risk factors into consideration. These factors include the profile of the accounting entity, the accounting entity's past inspection outcomes, complaints, intelligence and adverse news relating to any ML/TF offence involving the accounting entities or public accountants etc. In 2020, ACRA refined its risk assessment framework, using a 4-point risk bucketing approach based on key ML/TF risk information obtained through a sector wide survey, and gathered through its inspections of accounting entities. The risk assessment was refreshed again in end 2023.
- 8.7.9 ACRA has been conducting AML/CFT inspections on accounting entities to determine their compliance with AML/CFT requirements. Since the commencement of AML/CFT inspections, ACRA has inspected 396 accounting entities covering about 56% of the accounting entity population.¹¹⁷ Where AML/CFT breaches were uncovered, ACRA may take regulatory action against the public accountant or accounting entities. To-date, two accounting entities have been issued with a letter of advice, which is a form of disciplinary action under the Accountants Act. Advisories were issued to the other inspected accounting entities, there being no adverse findings which warranted sanctions. From 1 July 2023, further amendments were made to the Accountants Act and its subsidiary legislations to enhance ACRA's powers to conduct AML/CFT inspections on public accountants and accounting entities.

Other professional accountants (who are not public accountants)

- 8.7.10 Professional accountants i.e. ISCA members (including public accountants) are required to comply with the Ethics Pronouncement 200 (EP 200), which contains AML/CFT requirements on areas including CDD, record keeping and the filing of STRs. Since 1 July 2023, the EP200 has adopted the AML/CFT requirements which are in the Accountants (Prevention of Money Laundering and Financing of Terrorism) Rules 2023.
- 8.7.11 ISCA conducts a mandatory questionnaire as part of the annual ISCA membership renewal to monitor other professional accountants (non-public accountants) who provide services as scoped by the FATF.
- 8.7.12 Based on the questionnaire results, ISCA will risk-rate the relevant professional accountants and engage the higher-risk professional accountants (who are not public accountants) to assess if they are sufficiently aware of the AML/CFT obligations and obtain an understanding of the firm's AML/CFT internal policies, procedures and controls. ISCA will also recommend improvement plans and perform follow-up monitoring on the remediation actions taken relating to any non-compliance.
- 8.7.13 Based on the 2023 membership renewal results, 807 out of about 29,000 ISCA members (about 3%) declared that they perform services scoped by the FATF, of whom 756 (almost 95%) are under the purview of existing DNFBP supervisors (e.g. public accountants,

¹¹⁷ From 2015 to Dec 2023.

employees in accounting entities, CSPs which already come under ACRA's AML/CFT regulatory oversight). The remaining 51 members were further risk rated to determine prioritisation by ISCA for further engagement.

- 8.7.14 For professional accountants (who are not public accountants) found to be in breach of the EP 200 requirements, ISCA can initiate a complaints and disciplinary process to sanction them.

Outreach and engagement

- 8.7.15 ACRA works closely with ISCA and engages the sector in outreach events such as the ISCA Ethics Seminar and ISCA Practitioner Conference which are held regularly. For example, at the Ethics Seminar held in August 2019, the ISCA Ethics Committee shared an overview of the EP 200, as well as practical solutions to complying with the relevant AML/CFT requirements and STR filing. At the Ethics Seminar held in July 2022, STRO shared insights on the sector's suspicious transaction reporting. At the ISCA Practitioner Conference held in October 2022, there was an outreach effort to provide an overview of the sanctions landscape, risks relating to sanctions and proliferation financing, and ways for professional accountants to mitigate their sanctions risks.
- 8.7.16 ACRA also shared common findings and best practices from its EP 200 inspections through case studies in the 2018 Practice Monitoring Programme's Public Reports. To facilitate the sector's compliance with EP 200, ACRA also issues Audit Practice Bulletins. For example, in 2018, the Bulletin provided a CDD template form which accountants could use as part of their CDD process. This Bulletin was updated in July 2023 and continues to be regularly reviewed.
- 8.7.17 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls it has in place, the sector is assessed to be of low ML risk. ACRA will continue to apply an RBA to supervision over the sector and will focus on the supervisory framework implemented by ISCA over professional accountants. ACRA will also continue to engage the sector on relevant ML concerns and best practices.

8.8 PAWNBROKERS

Key exposures to ML threat areas

- 8.8.1 Pawnbroking refers to the business of lending money against the security of pledges. The industry caters to individuals who need short-term financial relief and possess valuables that can be pledged, e.g. PSPMs such as jewellery and luxury watches. The assets pledged can be redeemed anytime within the redemption period (which must be at least six months), and interest rates are capped by law to a maximum of 1.5% per month.
- 8.8.2 LEAs have observed a low number of cases involving the pawning of fraudulently obtained/stolen goods. These cases were observed to be straightforward and involved the monetisation of goods obtained via criminal conduct such as theft or misappropriation of another person's property. They were observed to be isolated instances of opportunistic crime and were not observed or known to be related to organised crime or ML activity.
- 8.8.3 The key threats arising from the sector largely relate to:
- (i) Pawnors repaying debts using illicit monies; and
 - (ii) Pawnors pawning fraudulently obtained/stolen goods.

Overall, the sector is assessed to be exposed to a moderate level of ML threat.

Vulnerability Assessment

Sector characteristics

- 8.8.4 The number of pawnbrokers has remained stable over the years, with 240 pawnbrokers as at the end of 2023 issuing loans worth approximately S\$7.1 billion.¹¹⁸ Currently, more than half of the pawnbrokers are run/owned by four companies listed on the Singapore Exchange.
- 8.8.5 Loans disbursed by pawnbrokers are domestic in nature, and disbursed to pawners who must be physically present at the pawnbroker to pawn their pledges. Hence, most of their customers are local residents, followed by foreigners working or residing in Singapore. The transactions performed are also straightforward, and are typically small in value, involving an average loan amount of S\$1,900. The sector's key vulnerability revolves around its cash intensity, and the potential illicit nature of the goods pledged. Given the largely face-to-face nature of pawnbroking, it has been observed that most pawnbroking loans are both disbursed and repaid in cash. All in all, the sector is assessed to be less vulnerable to ML.

AML/CFT controls within the sector

- 8.8.6 IPTO works closely with the Police to ensure that substantial shareholders and directors of pawnbrokers are fit and proper to carry on a pawnbroker business. This helps prevent criminals and their associates from controlling or engaging in pawnbroking activities.
- 8.8.7 Pawnbrokers are subject to AML/CFT requirements as set out in the Pawnbrokers Act 2015 (PBA), which are elaborated in the Information Guide on the Prevention of ML and CFT for pawnbrokers.¹¹⁹ The PBA requires pawnbrokers to conduct CDD on their customers who take a loan or make a transaction exceeding S\$20,000, in situations where there are grounds to suspect ML/TF involvement or where there is doubt as to the veracity or adequacy of the information collected in an earlier CDD process. This includes obtaining information on their SoW and SoF, as appropriate. Pawnbrokers are also required to monitor transactions and business relationships for suspicious activity and to file STRs and CTRs.
- 8.8.8 To address their key threats and vulnerabilities, pawnbrokers are required to take proactive and reasonable steps to ensure that the pledges have not been fraudulently obtained. If a pawnbroker reasonably suspects that an article has been obtained illegally, he has the power to seize the article and detain the person offering the article, and to deliver that person and the article into the custody of a Police officer.
- 8.8.9 IPTO adopts an RBA to supervision and assesses each pawnbrokers' risk profile to sieve out higher risk entities for inspection. In determining the risk profile, a broad range of risk factors is taken into consideration which includes the pawnbroker's transactional volumes and values of loans, its ongoing conduct, its accessibility to best practices, the presence of potentially adverse ML/TF information associated with the pawnbroker (including STRs filed against it) and the profile of its pawners. Based on its assessment of each pawnbroker's risk profile, it subjects higher risk pawnbrokers to more intensive supervisory scrutiny. This includes pawnbrokers at higher inherent risk of being misused for fraudulent pawning (e.g. pawnbrokers with a higher number of foreign customers). AML/CFT supervision performed by IPTO is focused on ensuring that pawnbrokers comply with AML/CFT requirements, including

¹¹⁸ This figure includes loans refinanced using the same collateral.

¹¹⁹ <https://rop.mlaw.gov.sg/files/Info%20Guide%202020%20for%20Pawnbrokers.pdf>

the requirement to conduct CDD (including on SoW and SoF, as appropriate), ensure proper record keeping and filing of STRs, CTRs etc.

- 8.8.10 In March 2020 and November 2023, IPTO also conducted surveys on its pawnbrokers to determine their level of AML/CFT knowledge and to sieve out weaker pawnbrokers for closer supervisory scrutiny. Through inspections conducted thus far, IPTO has observed that the pawnbrokers are generally compliant, except for some inadequacies in record-keeping, review of internal policies, procedures and controls, and training for employees. All deficiencies observed have been promptly rectified. IPTO has the power to impose administrative and criminal sanctions against pawnbrokers for any AML/CFT breach.
- 8.8.11 IPTO communicates with pawnbrokers through various channels such as inspections, industry briefings, and meetings with the Singapore Pawnbroker's Association. Through these channels, IPTO reminds the pawnbrokers of their latest risks, their AML/CFT obligations as well as IPTO's supervisory expectations. Other relevant AML/CFT guidance and information for pawnbrokers are also available on IPTO's website.
- 8.8.12 Overall, in consideration of the ML threats posed to the sector, its vulnerabilities as well as the strength of controls in place within the sector, the sector is assessed to be of lower ML risk. IPTO will continue to conduct risk-based inspections on pawnbrokers and engage them on AML/CFT concerns. IPTO has also observed that a number of pawnbrokers, including those under chain operators, have moved away from cash transactions and have adopted electronic/non-cash means for loan refinancing and/or payment of profits/interest. IPTO has been supporting the pawnbrokers in such endeavours by reviewing their proposed models and ensuring that they are in line with the PBA. IPTO will continue with its efforts on this front to reduce the sector's vulnerability to ML.

9. CONCLUSION

- 9.1 Singapore is committed to working closely with international and domestic stakeholders to prevent, detect, and enforce against ML. As an international business, financial and trading centre, Singapore must remain vigilant to the fast-evolving ML threat landscape and criminal methods and ensure that our AML regime and defences keep pace with these changes.
- 9.2 Singapore is therefore continually reviewing and enhancing our whole-of-system approach to preventing, detecting, and enforcing against ML to ensure that we have strong collective defences. Apart from enhancing our AML legal and regulatory framework and implementing close supervision of AML/CFT obligated entities across all sectors, the authorities in Singapore will continue to develop close partnership and collaboration between the public and private sectors to allow more timely identification and detection of risks and coordinated responses against identified risks.
- 9.3 This NRA provides a consolidated picture of the key national ML threats, risks, and vulnerabilities. FIs and DNFBPs should take into consideration this NRA as they develop and implement risks mitigation measures and strengthen their own AML defences.
- 9.4 The process of risks assessment is a dynamic one, and Singapore will continue to monitor and sense-make risks on an ongoing basis to ensure that our risks understanding, and risks mitigation measures remain up to date and effective.

ANNEX – SINGAPORE’S FREE TRADE ZONE REGIME

1. Singapore’s Free Trade Zones (FTZ) regime supports our position as a trade hub by streamlining customs formalities to facilitate efficient import, export and transshipment of goods through Singapore.
2. As a major transshipment hub, Singapore must continually balance streamlined regulation to facilitate efficient trade against adequate oversight to combat illicit activities.
 - a. Today, Singapore has 10 FTZs operated by three FTZ operators.
 - b. Singapore Customs works closely with each of the FTZ operators, as well as relevant local and international partners to ensure strong governance of the FTZs and combat any criminal misuse.
3. Over the years, Singapore Customs and its partners have identified new and evolving threats and challenges in managing our FTZs as the operating environment continues to change.
 - a. For instance, the risk of money laundering and/or terrorism financing (ML/TF) has grown over the years, alongside the growing sophistication of illegal actors.
 - b. Increased data visibility and risk profiling have also gained salience as important deterrents for trade-based money laundering (TBML).
4. Singapore Customs proactively adapted measures to address these challenges with its partners. Such measures include:
 - a. Effective enforcement. Since 2017, Singapore Customs has increased the frequency of risk-based inspections on warehouses in the various FTZs. The combination of regular and surprise checks helps to uphold high level of compliance among companies operating in the FTZs.
 - b. Regular reporting regime. The FTZ operators are required to submit monthly reports to Singapore Customs on any security-related incidents and suspicious activities. In turn, Singapore Customs also engages FTZ operators to raise awareness of money laundering or terrorism financing risks and their legal obligations in an FTZ. The two-way exchange facilitates timely detection of and action against criminal conduct.
 - c. Stringent security. Singapore Customs works closely with FTZ operators to ensure that security measures are up-to-date and effective. This includes expanding coverage of CCTV surveillance, and adoption of new security features such as biometric verifications, geo-fencing and real-time track-and-trace for personnel and vehicles entering the compound.
 - d. Sharpened risk profiling and assessment. Singapore Customs uses trade data from its National Single Window, TradeNet, to continually refine its targeting rules. These rules account for changes in the operating landscape, risk profiles of traders, risk alerts from agencies and international partners, as well as information from past cases. Customs officers also have access to data from FTZ Operators’ systems to

monitor cargo movements in and out of our FTZs. These have enabled Customs to flag goods-of interest for analysis and interventions, and aided Customs in numerous successful domestic and overseas seizures.

- e. Strong local and international partnership. Singapore Customs maintains an open channel with local and international partners to share actionable intelligence and operational support in tackling illicit activities in the FTZs. This partnership resulted in 56 successful seizures of illicit goods from 2016 – 2018. Customs also actively participates in a wide range of international joint operations yearly that span the targeting of tobacco, CITES goods, counterfeit goods, strategic goods and psychoactive substances.
5. Singapore Customs' efforts has been featured in the World Customs' Organisation's Practical Guidance on Free Zones, specifically for its involvement in the FTZs, use of data and IT systems, control and surveillance to detect/seize illegal goods in FTZs and cooperation.
 6. To further strengthen the safety and security of Singapore as a trade hub and to deter TBML/TF within our FTZs, Singapore Customs has also updated the relevant regulations following a comprehensive review of Singapore's FTZ regime.
 7. Singapore Customs' revised FTZ regime adopts a calibrated approach to tighten oversight and better ingrate trade data and systems, while minimising economic impact and compliance burden.
 - a. The major change is to introduce a licensing regime for FTZ operators, and mandate that these operators transmit advanced cargo information to Singapore Customs.
 - b. This change formalises the legal responsibilities of the FTZ operators. It also enhances visibility and oversight of cargo flowing through Singapore and enable Singapore Customs to be more targeted and effective at detecting illicit transshipments, including TBML cases, without unduly hindering legitimate economic activity.
 - c. The revised regime incorporates useful lessons from Singapore Customs' six-year Cargo Targeting System (CTS) trial, most notably on the need to (i) mandate timely submission of accurate and complete manifest data and (ii) have a robust system infrastructure to support information transmission to address concerns about system security and performance.
 - d. The revised regime is supported by updated FTZ legislation to bolster Singapore Customs' regulatory powers and clarify the penalty framework to deter illicit activity.
 8. To minimise potential disruption to the industry, Singapore Customs has been operationalising this revised regime by leveraging existing system infrastructure and incorporating key feedback from industry players.
 9. Singapore Customs is confident that the revised FTZ regime will strengthen Singapore's value proposition as a major transshipment hub that offers Governments and businesses alike efficiency, reliability, and security to meet their trading needs.