



# NATIONAL ASSET RECOVERY STRATEGY

**2024**  
**SINGAPORE**



# CONTENTS

<b>FOREWORD .....</b>	<b>2</b>
<b>INTRODUCTION: ASSET RECOVERY OBJECTIVES .....</b>	<b>4</b>
<b>PILLAR 1: DETECT suspicious and criminal activities, including the proceeds of crime and instrumentalities of crime .....</b>	<b>8</b>
1.1 Comprehensive Legal Frameworks .....	8
1.2 Effective Information Sharing Channels .....	8
1.3 Leveraging Technology and Data Analytics .....	10
1.4 Culture and Training .....	12
<b>PILLAR 2: DEPRIVE criminals of their ill-gotten proceeds through prompt seizure and confiscation .....</b>	<b>13</b>
2.1 Comprehensive Legal Frameworks .....	13
2.2 Robust and Swift Operational Response .....	14
2.3 International Cooperation and Partnerships .....	17
<b>PILLAR 3: DELIVER maximum recovery of assets for forfeiture and restitution to victims .....</b>	<b>21</b>
3.1 Asset Management .....	21
3.2 Restitution/Return to Victims .....	22
3.3 Loss Prevention .....	24
3.4 Alternative Measures .....	26
<b>Pillar 4: DETER criminals from using Singapore to hide, move, or enjoy their illicit assets. ....</b>	<b>28</b>
4.1 Updated and Effective Legal Frameworks .....	28
4.2 Public Education and Partnerships .....	29
<b>CONCLUSION .....</b>	<b>32</b>

## FOREWORD

**Singapore's success as an international financial, business, and trade hub is premised on our political and economic stability, strong rule of law, transparency in financial and other regulatory regimes, and vibrant financial ecosystem.** This is why investors are attracted to us. However, criminals will also try to exploit the same traits to launder their illicit funds.

Singapore is determined to preserve our hard-earned international reputation and credibility by taking a strong stance against money laundering (ML), and continually enhancing our Anti-Money Laundering (AML) regime.

**Asset recovery is one of the key priorities of our AML regime.** We seek to deprive criminals of their illicit gains, thereby removing the financial incentive for laundering their monies in Singapore. We also seek to provide recourse to victims of crime by helping them to recover property and assets lost to criminal activities. **Between January 2019 and June 2024, Singapore seized S\$6 billion linked to criminal and ML activities. S\$416 million has been returned to the victims, and S\$1 billion has been forfeited to the State.** The large bulk of the remainder is linked to ongoing investigations or court proceedings.

We are committed to continue enhancing our asset recovery regime, despite a sizeable proportion of money laundering cases being transnational in nature. These cases involve foreign predicate offences and foreign criminals who employ increasingly sophisticated and complex methods, including layering tactics, and digital technologies to conceal the movement of their illicit funds.

**Successful asset recovery requires a multi-faceted approach.** To this end, Singapore is launching our **National Asset Recovery Strategy**, focusing on the four operational pillars of **Detect, Deprive, Deliver, and Deter**. This strategy paper sets out a comprehensive national approach to asset recovery by making clear our asset recovery processes and roles of the various stakeholders in the Singapore ecosystem. The ecosystem comprises law enforcement agencies, sectoral regulators, private sector partners, and the public. Given the transnational nature of most ML-related activities in Singapore, **international cooperation**, including with foreign counterparts and international organisations such as INTERPOL, Egmont Group, and the Financial Action Task Force (FATF), is also key. Every partner plays a critical role in the global effort to identify, trace, seize, and return the proceeds of crime to their rightful owners, and hold the criminals accountable.

**We also need efforts upstream and a whole-of-society approach if we want to achieve better outcomes in loss prevention and minimise the harms to society.** For instance, the Anti-Scam Command under the Singapore Police Force, in collaboration with local banks, sent over 16,700 SMS warnings from March to April 2024 to more than 12,500 bank customers whom the authorities had detected were in the midst being scammed. This resulted in the disruption of more than 3,000 scams and averted losses of over S\$100 million. We also continue to build strong industry partnerships, such as Singapore's AML/CFT Industry Partnership, which is co-chaired by the Singapore Police Force and the Monetary Authority of Singapore.

We recognise, at the same time, that even the most robust preventive and asset recovery measures can be circumvented by determined and creative criminals. **Singapore will therefore continually enhance our regimes** to try our utmost to prevent criminals from exploiting Singapore's ecosystem, and upon detection, track them down and take them to task.



**PANG KIN KEONG  
PERMANENT SECRETARY  
MINISTRY OF HOME  
AFFAIRS**



**LAI WEI LIN  
SECOND PERMANENT  
SECRETARY  
MINISTRY OF  
FINANCE**



**CHIA DER JIUN  
MANAGING DIRECTOR  
MONETARY  
AUTHORITY OF  
SINGAPORE**

**CO-CHAIRS  
ANTI-MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM  
(AML/CFT) STEERING COMMITTEE  
26 JUNE 2024**

## INTRODUCTION: ASSET RECOVERY OBJECTIVES

1. **Singapore takes robust and strong actions against criminal activities, including financial crimes such as money laundering (ML). As an international financial, business, and trading centre and a responsible member of the international community, our dual objectives of building a dynamic, thriving hub, and maintaining a trusted system, are mutually reinforcing** – we do not trade off one against the other. Singapore is acutely aware that our openness and connectivity as an international financial, business, and trading centre could be exploited by criminals. Therefore, Singapore remains relentless in detecting and depriving criminals of their proceeds of crime while continuing to welcome legitimate businesses.
2. **ML and criminal activities are getting increasingly sophisticated, involving the swift movements of large sums of illicit proceeds and affecting sizeable numbers of victims across borders.** As an international trade, transport, and financial hub, Singapore is highly exposed to ML threats such as those arising from corruption, tax-ML, and trade-based ML. The rapid expansion of the digital economy in Asia, further accelerated by the COVID-19 pandemic, has led to the emergence of new ML and criminal typologies. These include virtual assets, cross-border digital payments, and cyber-enabled fraud, presenting new challenges for law enforcement agencies. Over the past four years, Singapore has witnessed an exponential surge in cyber-enabled fraud cases, particularly those orchestrated by overseas criminal syndicates. In 2023 alone, cyber-enabled fraud in Singapore resulted in a loss of S\$651.8 million. In addition, the growing ease of cross-border fund transfers has made it increasingly challenging to detect and trace the movement of criminal assets, as well as to swiftly freeze and recover them.
3. **Singapore adopts a Whole-of-Government (WOG) approach towards asset recovery.** There is strong commitment from all levels of the Government to tackle ML and criminal activities. We aim to prevent criminals from abusing our financial system, identify and trace criminals and criminal assets, and confiscate the assets to deprive the criminals of their illicit gains and provide restitution to the victims. To this end, Singapore has a comprehensive framework to holistically review and strengthen our Anti-Money Laundering (AML) regime. A WOG effort is led by an inter-agency AML/Countering the Financing of Terrorism (AML/CFT) Steering Committee (SC), which is supported by the Inter-Agency Committee (IAC) and the Risks and Typologies Inter-Agency Group (RTIG).<sup>1</sup> This work is supported by strong public-private partnerships such as the AML/CFT Industry Partnership (ACIP).<sup>2</sup> Refer to **Diagram 1** for the WOG ecosystem on AML/CFT. In addition, an Inter-Ministerial Committee on

---

<sup>1</sup> The AML/CFT SC, co-chaired by the Permanent Secretaries of the Ministry of Home Affairs (MHA) and the Ministry of Finance (MOF) and Managing Director of the Monetary Authority of Singapore (MAS), comprises more than 15 government agencies represented at a senior level. This ensures high-level policy direction and commitment to action across agencies on ML, Terrorism Financing (TF), and Proliferation Financing (PF) matters. The IAC is co-chaired by senior officials from MHA and MAS while the RTIG is led by officials from MHA and MAS.

<sup>2</sup> The ACIP, which is co-chaired by MAS and the Singapore Police Force (SPF), brings together relevant financial institutions (FIs) and other non-financial intermediaries.

Anti-Money Laundering (IMC-AML) was set up in 2023 to review Singapore’s AML regime.<sup>3</sup>

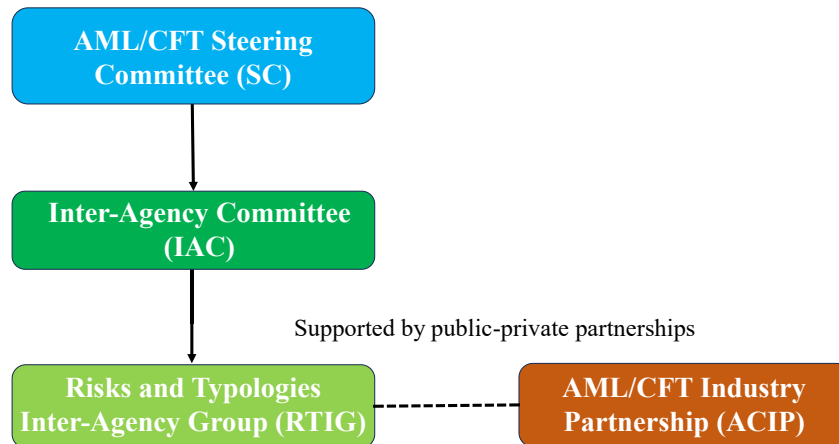


Diagram 1: WOG Ecosystem on AML/CFT

*Key Entities in Singapore’s AML Ecosystem*

- a) **The Singapore Police Force (SPF) is the primary agency investigating ML and other serious crimes.** Within SPF, the main departments involved in financial investigations are the **Commercial Affairs Department (CAD)** and the **Financial Investigation Branch (FIB) under the Criminal Investigation Department (CID)**. These departments conduct financial investigations, including identifying and tracing criminal assets, investigating ML and its predicate offences such as organised crime, unlicensed moneylending, cybercrime, and other specialised crimes like cyber-enabled fraud. SPF also supports other law enforcement agencies in ML investigations linked to other predicate offences, such as environmental offences, employment offences, illicit trafficking of health products, and tax offences.<sup>4</sup>

<sup>3</sup> The IMC-AML is chaired by the Minister in the Prime Minister’s Office and Second Minister for Finance and National Development, Ms Indranee Rajah, and comprises political office holders from the Monetary Authority of Singapore (MAS), Ministry of Home Affairs (MHA), Ministry of Law (MinLaw), Ministry of Manpower (MOM), and Ministry of Trade and Industry (MTI).

<sup>4</sup> The Immigration and Checkpoints Authority (ICA) enforces the Cross Border Cash Reporting Regime (CBCRR), with follow-up investigations by SPF where necessary; Singapore Customs investigates import/export offences; Ministry of Manpower (MOM) investigates employment offences; National Parks Board (NParks) and the National Environment Agency (NEA) investigate environmental offences; Health Sciences Authority (HSA) investigates illicit trafficking of health products; and the Inland Revenue Authority of Singapore (IRAS) investigates tax offences.

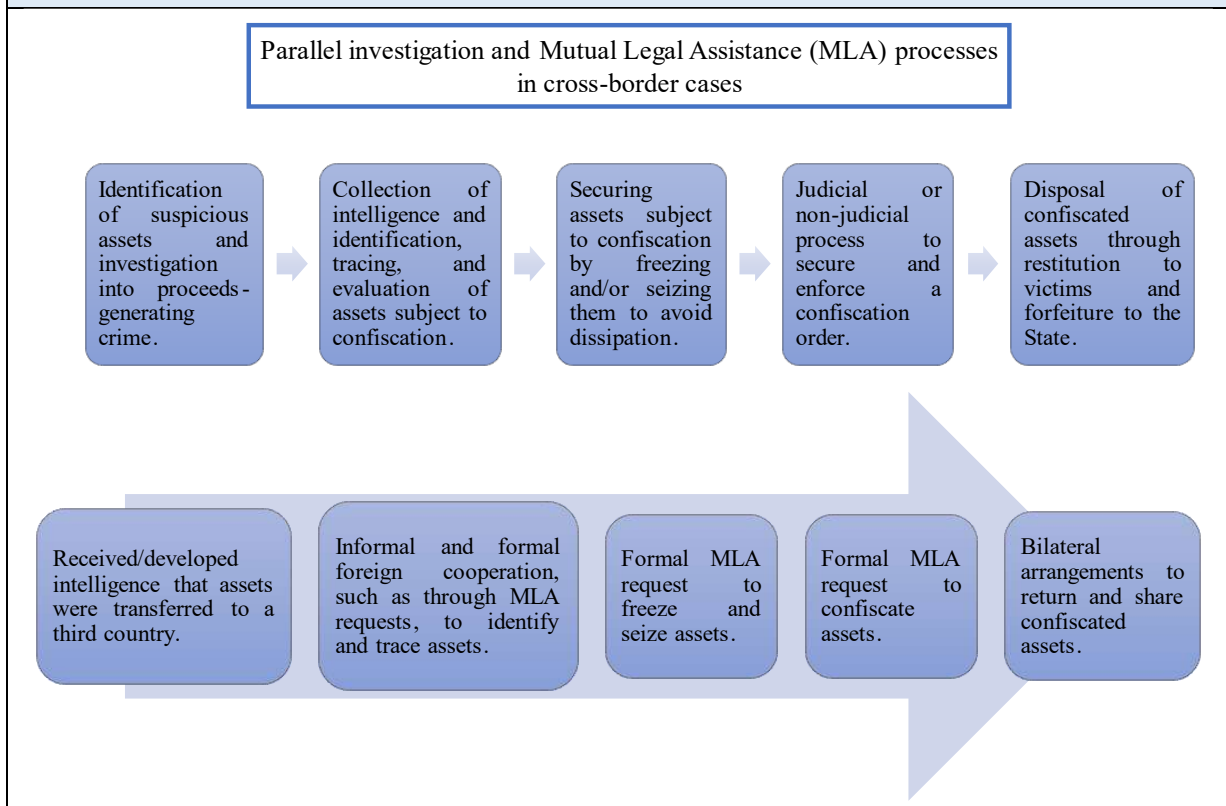
- b) **The Suspicious Transaction Reporting Office (STRO) of the CAD is Singapore's Financial Intelligence Unit (FIU).** STRO serves as Singapore's central agency for the receipt of disclosures filed by reporting entities, in the form of Suspicious Transaction Reports (STRs), Cash Movement Reports (CMRs), and Cash Transaction Reports (CTRs). STRO was established to detect and prevent ML, Terrorism Financing (TF), and other serious crimes by receiving and analysing these reports, then disseminating the analysis results to law enforcement agencies and AML/CFT regulators.
  - c) **The Central Narcotics Bureau (CNB) and the Corrupt Practices Investigation Bureau (CPIB)** are specialised agencies responsible for investigating ML offences linked to **drug and corruption offences** respectively.
  - d) The **Attorney-General's Chambers (AGC)** is led by the **Attorney-General**, who is also **the Public Prosecutor**, and has control over all criminal proceedings and conducts prosecution in court.
  - e) **Sectoral regulators**, such as the Monetary Authority of Singapore (**MAS**), Accounting and Corporate Regulatory Authority (**ACRA**), Council for Estate Agencies (**CEA**), and Urban Redevelopment Authority (**URA**), oversee Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) such as corporate service providers, real estate agents, and property developers.<sup>5</sup> They play an important role in ensuring that there are robust AML/CFT controls in their respective sectors, and **addresses any lapses in said controls**. Robust AML/CFT controls facilitate the detection of suspicious activities within these sectors. This, in turn, aids law enforcement agencies in detecting criminal activities and preventing the dissipation of illicit assets.
4. **Asset recovery is a fundamental tenet in Singapore's fight against ML and other crimes.** This sends a strong deterrence message that Singapore is determined to deprive criminals of their illicit gains. By doing so, it removes the key motivation for financial crime, while also providing reprieve for the victims. Maximising the recovery of criminal assets is a key aspect of the operating paradigm of law enforcement agencies. Refer to **Diagram 2** for the asset recovery framework in Singapore.

---

<sup>5</sup> MAS exercises supervisory responsibility over financial institutions and has in place regulations that impose AML/CFT requirements on them. The sectoral regulators for the non-financial sectors include: CEA for real estate agents and agencies; URA for property developers; ACRA for Corporate Service Providers and public accountants, and the Institute of Singapore Chartered Accountants (ISCA) for other accountants; Law Society of Singapore (LawSoc), in partnership with MinLaw, for lawyers; MinLaw for precious stones and precious metals dealers (PSMD); and Gambling Regulatory Authority (GRA) for casinos.

## Diagram 2 - Asset Recovery Framework in Singapore

Asset recovery is the process by which criminals or entities are **deprived of funds or other assets**, which are then **returned to victims or forfeited to the State**.



5. To this end, Singapore has launched our **National Asset Recovery Strategy**, comprising four operational pillars, namely:
- Detect** suspicious and criminal activities, including the proceeds of crime and instrumentalities of crime;
  - Deprive** criminals of their ill-gotten proceeds through prompt seizure and confiscation;
  - Deliver** maximum recovery of assets for forfeiture and restitution to victims; and
  - Deter** criminals from using Singapore to hide, move, or enjoy their illicit assets.



## **PILLAR 1: DETECT suspicious and criminal activities, including the proceeds of crime and instrumentalities of crime**

### **1.1 Comprehensive Legal Frameworks**

**1.1.1 Singapore has a comprehensive suite of laws to detect and trace suspicious criminal and ML activities, networks of criminals, and movement of illicit funds.** These enable law enforcement agencies to detect and disrupt criminal activities and deprive criminals of their illicit proceeds, and to empower sectoral regulators and other government authorities to take appropriate regulatory actions.

- a) **Section 20 of the Criminal Procedure Code (CPC)** empowers SPF, CNB, and CPIB officers to **order any individual or entity to produce information, documents, or items** for a criminal investigation. This enables them to detect and trace criminal properties of individuals and companies.
- b) **Section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA)** sets the legal obligation for any persons / entities to **file STRs to STRO** if they know or have reasonable grounds to suspect that any property is linked or intended to be used in connection with a criminal activity.
- c) **Anti-Money Laundering and Other Matters Bill in 2024 (Upcoming)** seeks to strengthen the ability of sectoral regulators to access STRs filed by their regulated entities to enhance AML/CFT monitoring and detection.

### **1.2 Effective Information Sharing Channels**

**1.2.1 Singapore has in place coordination platforms to facilitate regular and timely sharing of information and identification of ML and predicate offence risks among government agencies and with private sector stakeholders, including FIs.** These platforms enable stakeholders to better detect risks and potentially illicit assets, share information with the relevant authorities in a timely manner to trigger investigations, thereby enhancing asset recovery. Government agencies and industry partners also work closely through the following platforms and mechanisms to identify networks of criminal and ML syndicates and trace the movement of illicit funds.

- a) The **Risks and Typologies Inter-Agency Group (RTIG)** – oversees the identification, assessment, and mitigation of existing and emerging ML, TF, and Proliferation Financing (PF) risks at the WOG level. The RTIG comprises all relevant supervisory, regulatory, law enforcement and policy agencies, and STRO; it facilitates the review of ML/TF/PF enforcement policies, information sharing, and coordination on ML/TF/PF cases.
- b) The **AML/CFT Industry Partnership (ACIP)** – brings together the financial sector, law enforcement agencies, and other government entities to collaboratively identify, assess, and mitigate key and emerging ML and TF risks faced by Singapore through public-private partnership initiatives (refer to **Box Story 1**).

## Box Story 1

**In 2020, SPF observed a spate of Business Email Compromise frauds that targeted victims outside Singapore and utilised bank accounts in Singapore to receive the criminal proceeds.** SPF's investigations uncovered a network of **Singapore-incorporated companies** which were suspected to be receptacles awaiting deployment for ML.

Criminals used several corporate service providers (CSPs) in Singapore that provided incorporation and nominee director services. These CSPs were found to have assisted foreign parties to incorporate shell companies in Singapore. **114 companies were found to be linked to complaints of crime, and over US\$84 million (approximately S\$113 million) of criminal proceeds were transferred into bank accounts in Singapore held by these companies between August and December 2020.**

**SPF worked closely with STRO, foreign law enforcement agencies, including the United States (US) Federal Bureau of Investigation, and local banking partners in ACIP to promptly identify bank accounts suspected to be under the control of criminals and took pre-emptive actions to prevent further losses of at least US\$20 million (approximately S\$27 million) from victims. Over US\$33 million (approximately S\$44 million) in criminal proceeds were seized from the shell companies' bank accounts, with more than US\$10 million (approximately S\$13 million) returned to the victims.**

To enhance industry awareness of this emerging ML typology, SPF, MAS, and ACIP jointly issued an ACIP advisory on the typology, red flag indicators, and mitigating measures. MAS and ACRA have also subjected the relevant banks and CSPs to enhanced supervision and monitoring.

- c) **Collaborative Sharing of ML/TF Information and Cases (COSMIC)** was launched by MAS on 1 April 2024 to facilitate the sharing of risk information among key financial institutions via a secure platform, for better detection of ML/TF/PF risks.<sup>6</sup>

---

<sup>6</sup> COSMIC allows financial institutions to securely share information on customers who exhibit multiple “red flags” that may indicate potential financial crime concerns. COSMIC currently focuses on three key financial crime risks in commercial banking, namely: misuse of legal persons, misuse of trade finance for illicit purposes, and PF.

## 1.3 Leveraging Technology and Data Analytics

**1.3.1 Singapore actively leverages technology and data analytics to enhance the detection and tracing of criminal syndicates, criminal assets, and movement of illicit funds.** This has enabled law enforcement agencies to deal more effectively with increasingly sophisticated criminals employing more complex layering tactics to conceal their criminal activities.

- a) **Project Production Orders: Electronic Transmission (POET)** is a digital interface between local law enforcement agencies and banks to **enable expeditious access and retrieval of banking information**. This enables investigators to quickly form a financial profile of the subject or trace the movement of funds, and support banks in conducting faster analysis of suspicious customers/transactions (refer to **Box Story 2**).

### Box Story 2

Launched by SPF in 2019, **Project POET is a public-private partnership that uses technology and automation to expedite the transmission of banking information from banks to law enforcement agencies for domestic investigations.** This enables investigators to obtain such information in just a **fraction of the time previously required (reducing it from 10 to 90 days in extreme cases to one day)**. Covering five banks in Singapore (OCBC, DBS, UOB, SCB and Maybank), the process involves law enforcement agencies sending a standardised electronic production order to the banks, whose systems automatically retrieve the relevant banking information and return them to law enforcement agencies electronically.

**Project POET has empowered investigators to apply analytical tools directly to electronic data, tailored to their investigative requirements.** This enhancement has bolstered law enforcement agencies' investigative capabilities, resulting in more efficient investigations and expedited tracing of illicit assets. Furthermore, it has generated efficiencies and cost savings for the involved financial institutions by eliminating manual processes. Recognising Project POET's role in harnessing technology and the private sector to combat crimes, SPF was awarded the **Public/Private Partnership Award (Public Sector) in the 2021 WITSA Global ICT Excellence Awards**. SPF aims to expand this initiative by onboarding more banks to the system.

- b) In 2022, STRO commissioned its analytics and data management system, enhancing **its capabilities to process large volume of reports on suspicious financial activities and improve the quality of financial intelligence** disseminated to law enforcement agencies and regulators. Law enforcement agencies and regulators can also **leverage the financial intelligence available in STRO's database** for their investigations (refer to **Box Story 3**).

### **Box Story 3**

**STRO identified a network of over 40 individuals whose bank accounts appeared to be controlled by a syndicate.** The bank accounts shared a common mailing address in another country, and the accounts were opened online and authenticated via the Singpass MyInfo channel, Singapore's digital identity online data repository.

**Data analytics were used to analyse the STRs on the group, leading to the discovery of a large network comprising hundreds of individuals and bank accounts from multiple banks.** STRO's analysis revealed that some account holders had the same contact numbers and similar public domain email addresses. The bank accounts were also operated from the same or common electronic devices. Since some bank accounts had received proceeds from scams, these individuals were suspected to be money mules involved in possible scam activities.

As STRO's analysis revealed that there were a handful of potential money mules whose bank accounts had yet to be used to receive funds from victims of various scams, **STRO collaborated with relevant stakeholders to proactively take down the syndicate.** The Anti-Scam Command conducted an operation to apprehend the money mules and disrupt the scammers from using the bank accounts of these individuals to perpetrate their crimes.

## 1.4 Culture and Training

### 1.4.1 Recognising that every investigator or prosecutor plays a critical role in tackling crimes and asset recovery, Singapore pays particular attention to the competency development and training of our officers.

- a) SPF Investigation Officers undergo training for financial investigations, guided by a financial investigation competency framework with varying levels of competencies based on job functions. Investigation Officers handling white collar crimes attend specialised courses to equip themselves with the necessary knowledge and techniques, including leveraging financial intelligence in their investigations (refer to **Box Story 4**).

#### **Box Story 4**

**The massive ML case in 2023, which saw more than S\$3 billion of assets seized or frozen, involved comprehensive intelligence gathering and thorough operation planning.** SPF launched a comprehensive and coordinated intelligence probe after receiving information, including STRs, on suspicious activities, such as the use of suspected forged documents to substantiate sources of funds in bank accounts in Singapore. To develop as full a picture as possible of the suspects, and their associates, their suspected criminal activities, and their assets, SPF painstakingly and discreetly investigated the web of suspects and traced their assets. **More than 400 SPF officers conducted simultaneous raids at multiple locations island-wide on 15 August 2023 to arrest and seize the assets of 10 suspects.**

**The multi-agency effort resulted in the freezing or seizure of criminal assets estimated at more than S\$3 billion,** including seizures of monies in bank accounts amounting to more than S\$1.45 billion, cash (including foreign currencies) amounting to more than S\$76 million, and cryptocurrencies of more than S\$38 million.

As of June 2024, about S\$944 million, or more than 90 per cent of the seized assets from the 10 convicted subjects, had been forfeited to the State. The case is ongoing against 17 other persons who are not in Singapore. SPF will maintain the prohibition against disposal and custody of the seized assets associated with these individuals until the assets are dealt with by the Court at the conclusion of the case.

- b) AGC and law enforcement agencies have curated training programmes, Standard Operating Procedures (SOPs), and guidelines to ensure that investigators proactively identify and locate criminal assets and proceeds of crime during seizure raids. This plays a critical role in preventing criminal asset dissipation and facilitating subsequent asset recovery. Prosecutors are also trained on court procedures relating to disposal and confiscation orders for seized criminal assets and proceeds. These skillsets are constantly refined and put into practice in the investigation of ML and criminal cases.

## **PILLAR 2: DEPRIVE criminals of their ill-gotten proceeds through prompt seizure and confiscation**

### **2.1 Comprehensive Legal Frameworks**

**2.1.1 Singapore possesses a comprehensive array of laws designed to swiftly and effectively deprive criminals of their illicit proceeds, whether situated domestically or abroad.** Our law enforcement agencies have access to various legal provisions throughout the stages of criminal investigation and asset recovery, tailored to the specifics of each case's circumstances.

#### Seizure

- a) **Section 35 of the Criminal Procedure Code (CPC)** is the main legal provision empowering Singapore's law enforcement agencies to **promptly seize, or prohibit the disposal of, or deal with suspected criminal or stolen property** and instrumentalities of crime without a Court order, aiming to **prevent asset dissipation**.
- b) This is complemented by **Sections 19 to 21 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA)**, which empower the **Courts to issue restraint and charging orders for property** that may be **subject to confiscation once proceedings have been instituted**. These orders prevent any dealing, transfer, or disposal of property subject to confiscation.
- c) Additionally, **CPIB officers** are empowered under **Section 22 of the Prevention of Corruption Act (PCA)** to restrain or seize any property pertaining to corruption-related offences under the PCA and the Penal Code. **CNB officers** are empowered under **Sections 24 and 26 of the Misuse of Drugs Act (MDA)** to seize and detain any property liable to seizure when conducting searches into any place or premises.
- d) For other **predicate offences**, the relevant law enforcement officers have seizure powers under other Acts such as the **Customs Act, Immigration Act, and Gambling Control Act**.

#### Confiscation and Disposal

- a) **Section 364 of the CPC** empowers the Courts to **order the disposal of property** at the end of a proceeding, including **the forfeiture and confiscation of property laundered or proceeds of ML**.
- b) The **CDSA** provides additional legal tools for the **Courts to issue confiscation orders for criminal assets that are not directly linked to an offence**.
- c) **Section 64 of the CDSA** enables the Courts to, on the application of the Public Prosecutor, make a confiscation order against a person convicted of a Cross Border Cash Reporting Regime offence for any sum exceeding the prescribed amount of S\$20,000.

- d) **Sections 40 and 41 of the Gambling Control Act** allow the Courts to **order the forfeiture of property used in the commission of gambling offences**.
- e) The **Organised Crime Act** provides for the **civil confiscation of benefits** derived from organised crime activities **without a conviction**.
- f) **Section 370 of the CPC** provides for the disposal of property when **no court proceedings have commenced**. There is **judicial oversight** through mandatory reporting to the Courts one year from the date of seizure if the seized property is no longer relevant to investigations. If the property is to be disposed of and there are **no claimants to the right of ownership, it would be forfeited to the State**.
- g) Apart from the above-mentioned provisions in the CPC, **CNB officers** can also exercise the powers under **Sections 28 and 29 of the MDA to dispose of assets**.

## **2.2 Robust and Swift Operational Response**

### **2.2.1 Singapore has sharpened operational responses and coordination among both law enforcement and prosecution agencies to effectively deprive criminals of their illicit proceeds and facilitate asset recovery.**

- a) In 2018, the **Inter-agency STR Analytics Team (ISTRA)** was established to facilitate **operational and enforcement coordination at the WOG level**, including for more sophisticated ML cases. We are currently enhancing ISTRA to enable more proactive upstream surveillance, monitoring, and disruption of ML threats and criminal proceeds across sectors of the economy with higher ML risks. This enhancement facilitates improved synchronisation efforts among relevant agencies to prevent criminals from laundering their illicit proceeds through the Singapore ecosystem. It strengthens downstream seizure, confiscation, and deprivation of criminals proceeds through comprehensive mapping of criminal networks and their assets in preparation for coordinated inter-agency operations.
- b) **Joint SOPs** between SPF and respective law enforcement agencies have been established and are regularly refreshed to ensure seamless coordination between agencies and facilitate parallel ML and sectoral regulatory investigations. There is a **strong focus on asset recovery in the entire criminal investigation process** from seizure, confiscation, to disposal of criminal assets, taking into consideration evolving ML and criminal typologies (refer to **Box Stories 5 and 6**).

## Box Story 5

In the S\$3 billion ML case, SPF seized a range of criminal assets including:

- 207 properties
- 77 vehicles
- 483 luxury bags
- 169 luxury watches
- 580 pieces of jewellery
- Thousands of bottles of liquor and wine
- 68 gold items including gold bars
- Bearbrick figurines
- More than S\$38 million of cryptocurrency
- More than S\$1.4 billion in bank accounts
- S\$76 million in physical cash

### *Photographs of seized assets*

#### Luxury bags



#### Liquor and wine



#### Luxury watches and jewellery



#### Bearbrick figurines





### Box Story 6

**On 15 August 2023, SPF conducted a large scale, island-wide raid as part of its investigations into a group of foreign nationals suspected of laundering the proceeds of their overseas organised crime activities into Singapore. During this raid, 10 foreign nationals were arrested, including Su Haijin (“Su”), a 41-year-old Cypriot national.**

Investigations revealed that **Su was involved in unlawful remote gambling activities abroad.** The charges against Su mainly concerned **Yihao Cyber Technologies Pte Ltd (“Yihao Cyber Technologies”), a Singapore-incorporated company owned by Su.** Between January and October 2021, Yihao Cyber Technologies received payments from an overseas company involved in remote gambling operations targeting foreign nationals, deriving revenue from such operations. These payments formed part of the monies that were held in **Yihao Cyber Technologies’ bank accounts, totalling S\$999,920.00 and S\$438,947.20 across two banks.** Despite being the director and sole shareholder of Yihao Cyber Technologies, Su was unable to account satisfactorily that these sums received in the company’s bank accounts were from legitimate sources. Investigations showed that the company did not have any legitimate business operations in Singapore.

**On 4 April 2024, Su was convicted and sentenced to 14 months’ imprisonment** for one count of resistance to lawful apprehension under Section 225B of the Penal Code and two counts of ML under Section 55 of the CDSA. The remaining charges against him were taken into consideration for sentencing.

The State Court also ordered the **forfeiture of more than S\$165 million (or about 95 per cent) of the assets seized** from Su, his wife, and his companies.

- c) Our law enforcement agencies also employ **Concealed Income Analysis (CIA)** in ML and predicate investigation cases, conducted by qualified in-house accountants. This supports the **confiscation of criminal assets** that could not be supported and explained by known sources of income of the criminal actors (refer to **Box Story 7**).

### Box Story 7

In an investigation conducted by SPF, Heng Ee Howe (“Heng”), a 60-year-old Singaporean man, was sentenced to **three months’ imprisonment and a fine of S\$360,000** on 2 March 2018 for assisting in carrying out a public lottery and managing remote gambling by others, facilitated through the receipt of bets via instant messaging platforms. On the same day, Heng’s wife, Tin Suh Chyong (“Tin”), a 55-year-old Singaporean woman, was also sentenced to **two weeks’ imprisonment and a fine of S\$100,000** for offences under the Common Gaming Houses Act and Remote Gambling Act.

In June 2015, SPF arrested Heng and Tin on suspicion of offences under the Remote Gambling Act. Subsequently, parallel predicate and financial investigations were initiated for possible ML offences.

SPF investigations revealed that Heng was involved in the unlawful collection of 4D bets on behalf of “Ah Gu”, a member of a gambling syndicate, with Tin’s assistance. Heng received commissions from a portion of the total bet amounts and punters’ winnings. Upon receiving the bets, Heng consolidated and transmitted the bets to Malaysian runners, whose contact information was provided by “Ah Gu”. Tin aided Heng in consolidating and transmitting bets to the Malaysian runners when Heng was unavailable.

The **prosecution successfully secured a Restraint Order on Heng and Tin’s bank accounts and a Charging Order under the CDSA on their condominium unit to prevent dissipation of the properties while** financial investigations into Heng and Tin were ongoing.

**Concurrently, an in-house Chartered Accountant at SPF conducted a concealed income analysis as part of parallel financial investigations, scrutinising Heng’s and Tin’s financial records for the five years preceding their arrest.** Upon reviewing their assets, liabilities, legitimate income, and expenses during this period, it was determined that **Heng and Tin had amassed unexplained wealth totalling S\$1,093,246.92 and S\$29,669.81**, respectively, between 1 June 2010 and 3 June 2015. These sums were **disproportionate to their known sources of income.** Consequently, SPF sought a confiscation order against Heng and Tin to forfeit the entire illicit income amounting to S\$1,122,916.73.

On 15 January 2019, **Heng and Tin were ordered by the Court to pay a sum of S\$1,093,246.92 and S\$29,669.81, respectively, to the Government, representing benefits that were believed to have been derived from their illegal betting activities.**

## 2.3 International Cooperation and Partnerships

### 2.3.1 Singapore actively collaborates with foreign partners to deprive criminals of their ill-gotten gains, including criminal proceeds derived from foreign crimes.

- a) **Singapore leverages the Mutual Assistance in Criminal Matters Act (MACMA) for cooperation in criminal and asset recovery matters with foreign counterparts.** Under the MACMA, Singapore can provide Mutual Legal Assistance (MLA) to another jurisdiction, including sharing information to facilitate the investigation and prosecution of ML and predicate offences, enforcement of foreign confiscation orders, as well as search and seizure of items. Between 2019 and 2023, Singapore received 905 incoming MLA requests from, and made 204 MLA requests to, foreign counterparts pertaining to ML and predicate offences.
- b) **Our law enforcement agencies adopt a proactive approach in targeting illicit money flows through Singapore.** Cognisant that criminals might exploit Singapore’s openness as an international financial, trading, and transportation hub, our law enforcement agencies actively commence domestic ML investigations into cases surfaced by foreign counterparts to identify any potential nexus to Singapore. SPF also proactively engages its foreign counterparts to alert them to the presence of criminal proceeds, and where appropriate, conducts joint investigations when

there is a nexus to Singapore, regardless of whether Singaporeans were victims (refer to **Box Story 8**).

### **Box Story 8**

**On 24 May 2023, a Singaporean male, M J-Earn Joesz (“M J”), was sentenced to four months and two weeks’ imprisonment and a S\$6,000 fine for conspiring to launder fraudulent Value-Added-Tax (“VAT”) refunds from the United Kingdom (UK), breaching Customs declaration obligation under the Customs Act 1960 and the Goods and Services Tax (GST) Act 1993.**

**This prosecution arose from joint investigations** conducted by SPF and the Singapore Customs, with the assistance of HM Revenue and Customs of the UK (“HMRC”), **following information received of an unsuccessful attempt to make VAT refund claims in another unrelated European country.**

Around December 2020, M J, along with several other individuals, was recruited by a Singaporean, Yeo Alan, to travel to London to collect fake jewellery and claim VAT refunds for said jewellery. M J successfully obtained a VAT refund totalling EUR 30,940 (approximately S\$44,650) and transported the sum from London to Singapore. However, upon his arrival in Singapore, M J failed to declare the jewellery and did not pay the GST leviable on the jewellery. In collaboration with HMRC and Singapore Customs, SPF arrested M J in Singapore on 12 December 2022.

**The mastermind, Yeo Alan, was eventually convicted for conspiring with M J to launder fraudulent VAT refunds and was sentenced to eight months’ imprisonment on 14 April 2023.**

- c) **STRO, as Singapore’s FIU, proactively exchanges financial intelligence with foreign FIU counterparts to develop leads with the aim of furthering ML/TF investigations.** STRO can exchange financial information with FIUs in the Egmont Group without the need for a Memorandum of Understanding (MOU) or Letter of Undertaking (LOU), as long as the safeguards for the use and confidentiality of the information are secured through an undertaking by the foreign authority. This allows for expeditious information exchanges with STRO’s foreign counterparts. As of March 2024, there are 174 Egmont members, including Singapore. Law enforcement agencies may also tap on STRO’s network of foreign FIUs to seek financial intelligence to further their ML/TF investigations (refer to **Box Story 9**).

### Box Story 9

STRO received a STR filed concerning Person A, a homemaker, whose source of wealth was derived from a divorce settlement with her former husband, Person B. Person B's source of wealth was allegedly derived from his role as a hedge fund manager and senior figure at Company C, a hedge fund company. The STR indicated that Company C's bank account was allegedly used as a conduit for receiving and transferring proceeds linked to foreign tax evasion.

STRO observed that Country D was investigating an alleged fraud exceeding €22 million (approximately S\$37.3 million), involving Persons A, B, and other entities. The fraud pertained to the refund of dividend withholding tax by Country D. Person B was identified as the main representative of the pension funds that submitted applications for withholding tax refunds. **STRO proactively shared information on Person A with the FIU of Country D.**

Given the indications that a potential ML offence involving foreign tax evasion, may have occurred in Singapore through Person A, **STRO conducted an analysis and disseminated its findings to the relevant domestic law enforcement agency. This prompted the initiation of a ML investigation in Singapore, resulting in the seizure of approximately £12.9 million (approximately S\$21.9 million) and US\$7.9 million (approximately S\$10.7 million) from Person A in Singapore.**

**2.3.2 On the multilateral front, Singapore leverages multilateral platforms such as INTERPOL's Global Rapid Intervention of Payments (I-GRIP), Egmont Group, and Asset Recovery Interagency Network Asia Pacific (ARIN-AP) for asset recovery efforts.** These include using stop-payment mechanisms on these platforms to trace, intercept, and freeze the flow of criminal proceeds across borders. STRO also taps on the Egmont Group's Rapid Response Program and the Financial Intelligence Coordination Group (FICG)'s Regional Fraud Response mechanism to expedite information sharing relating to cyber-enabled fraud between FIUs, law enforcement agencies and FIs, to enhance the chances of asset recovery (refer to **Box Stories 10 and 11**).

### Box Story 10

SPF actively participates in internationally coordinated operations against scams. **In 2023, the Anti-Scam Command participated in two such operations.** The first was **INTERPOL's Operation First Light**, which involved more than 76 countries. During the operation, **over 2,000 individuals were investigated, and over 5,300 bank accounts were frozen in Singapore, resulting in the recovery of more than S\$11.5 million.** Additionally, the Anti-Scam Command **seized virtual assets worth more than S\$30 million.**

The second was **INTERPOL's Operation HAECHI**, which involved 32 countries. During the operation, the Anti-Scam Command **investigated more than 800 suspects involved in scams and ML, blocked more than 4,900 bank accounts, and seized over S\$16.4 million in Singapore.** Additionally, the Anti-Scam Command **blocked more than 300 virtual accounts and seized over S\$500,000 in virtual assets.**

### **Box Story 11**

**STRO actively participates in the Financial Intelligence Consultative Group (FICG)**, a regional body comprising FIUs from Southeast Asia, New Zealand, and Australia. The FICG aims to strengthen collaboration on AML/CFT by prioritising and addressing regional risks and facilitating the sharing of intelligence.

**Currently, STRO is co-leading a project** under the FICG, along with the FIUs from Malaysia (UPWBNM) and Indonesia (PPATK). Together, they have **developed a regional fraud response mechanism to enhance operational collaboration in combatting cyber-enabled fraud and expedite information sharing relating to scams in the region.**

#### **2.3.3 Singapore also plays an active role in driving the global asset recovery agenda.**

During Singapore’s FATF Presidency (from 1 July 2022 to 30 June 2024), the FATF spearheaded initiatives to strengthen global standards on asset recovery. These initiatives required countries to enhance their laws to include the quick freezing of illicit funds and promote international cooperation. Additionally, the FATF reinforced the international framework for transparency of beneficial ownership of legal persons and arrangements, making it more difficult for criminals to hide their assets. To facilitate practical implementation of strategies and foster the exchange of best practices, Singapore collaborated with the FATF and INTERPOL to co-host two rounds of the FATF-INTERPOL Roundtable Engagement on Asset Recovery in 2022 and 2023 (refer to **Box Story 12**).

### **Box Story 12**

**Singapore partnered with the FATF and INTERPOL to launch the inaugural FATF-INTERPOL Roundtable Engagement (FIRE) initiative in 2022.** This initiative aims to bring greater global focus on efforts to **enhance asset recovery** amidst the evolving financial crime threat landscape. FIRE I was held in Singapore in 2022, followed by FIRE II in Lyon, France, in 2023.

**FIRE I (2022) and FIRE II (2023) collectively saw the participation of over 350 experts** from law enforcement agencies, asset recovery offices, FIUs, prosecutors, regulators, policy makers, industry experts, and think-tanks from across the world. Through thematic panel discussions and real-life case studies that covered the end-to-end asset recovery process, participants had the opportunity to discuss and explore practical ways to enhance asset recovery and international cooperation. SPF presented on Singapore’s approach and strategy for effective asset management at both FIRE I and FIRE II. Many attendees described FIRE as a “timely and authentic forum” where participants could come together to explore practical operational solutions related to asset recovery.

### **PILLAR 3: DELIVER maximum recovery of assets for forfeiture and restitution to victims**

- 3. Singapore adopts a victim-centric approach towards asset recovery.** When identifiable victims are present in a criminal investigation, our priority is to return the confiscated assets to the rightful owners. However, in instances where no identifiable victims exist, we prioritise forfeiting the criminals' illicit gains to the State.

#### **3.1 Asset Management**

**3.1.1 To maximise the return of assets to victims, Singapore prioritises the preservation of seized and/or confiscated criminal assets' value through effective asset management.** Upon the seizure of criminal assets or properties, law enforcement agencies preserve their value through adherence to **common asset management SOPs**. These agencies are responsible for overseeing the upkeep and value preservation of the seized assets, including engaging specialised services from **industry partners or service providers to manage assets that are highly depreciative**, particularly if not kept in specified conditions. Such assets may include luxury items such as fine art, antiques, investment-grade wine, vessels, and animal livestock like exotic fish, reptiles, and racehorses.

**3.1.2 In addition, law enforcement agencies will try to promptly dispose of highly depreciative seized and/or confiscated assets to preserve their monetary value.** Recognising that court proceedings for sophisticated ML and predicate cases may be protracted, and the management of seized assets during these proceedings may incur significant costs for certain types of property, Singapore is **planning to amend Section 35 of the CPC and introduce a new Section in the CDSA**. These amendments seek to empower law enforcement officers to apply to the **Courts to order the sale of seized assets that significantly depreciate or have high maintenance costs before the conviction** of the cases.

**3.1.3 For forfeiture to the State, non-cash criminal assets may be sold through auctions. The proceeds from the sale of forfeited criminal assets, along with any forfeited cash, will be deposited into the Consolidated Fund, which is centrally managed by the Accountant General's Department, on behalf of the Singapore Government.**

**3.1.4 AGC and law enforcement agencies are continually improving our approach to managing new types of seized criminal property.** New SOPs have been developed and refreshed for the freezing, seizure, management, and disposal of crypto-assets, which are increasingly prevalent in ML and predicate cases.

- a) **In 2023, AGC established two specialised task forces to combat technology-enabled and technology-facilitated crimes: the Technology Crime Task Force and the Cryptocurrency Task Force.** The former addresses computer or technology-assisted crimes and handles digital evidence, while the latter focuses on matters pertaining to cryptocurrencies as assets, including assisting SPF in tracking and handling such assets. Each team comprises approximately 20 prosecutors who have received training in handling digital evidence and

understanding the nuances of technology-related criminal activities. Task force members also collaborate with relevant government agencies such as SPF (CID and CAD) and receive specialised training, including overseas training opportunities.

- b) Beyond the specialised task forces, **all prosecutors in AGC are required to undergo basic training in technology crimes and digital evidence**. This is essential as criminals are increasingly utilising technology for a wide spectrum of crimes. Additionally, AGC collaborates closely with major technology companies and social media firms to combat cybercrime and address challenges posed by technological advancements.

### 3.2 Restitution/Return to Victims

- 3.2.1 Singapore takes proactive steps to engage with foreign partners and the private sector to return recovered assets to the rightful jurisdictions and entities.** Recognising that criminals may exploit Singapore's open economy to launder illicit proceeds from foreign and/or cross-border crimes, Singapore seeks to return seized criminal assets in convicted cases where links to foreign crimes and/or cross-border syndicates were established (refer to **Box Stories 13, 14, and 15**).

#### Box Story 13

**Vincent Ramos, Chief Executive of Canada-based Phantom Secure, and four of his associates were indicted by a federal grand jury in the US in March 2018** on charges related to operating a criminal enterprise facilitating the **transnational importation and distribution of narcotics. This was achieved through the sale and service of encrypted telecommunications devices and services.**

US authorities shared information with SPF regarding funds in Singapore suspected to be Ramos' criminal proceeds. **This allowed SPF to initiate investigations at an early stage. Upon receiving an MLA request from the US authorities, SPF promptly seized approximately US\$3.5 million (approximately S\$4.7 million) from a corporate bank account within a day.** SPF's financial investigations further revealed three other corporate bank accounts suspected to contain Ramos' criminal proceeds, which were swiftly seized to prevent their dissipation.

Information gathered by SPF was shared with the US authorities, leading to all four bank accounts being subjected to a forfeiture order issued by the US Court. **In December 2020, seized funds totalling about US\$3.8 million (approximately S\$5.1 million) across four corporate bank accounts in Singapore were repatriated to the US authorities.**

#### **Box Story 14**

In May 2016, SPF assisted the Ministry of Public Security (MPS) of the People's Republic of China (PRC) in conducting asset tracing in Singapore as part of their investigation into Ezubao, a large-scale Ponzi scheme. This scheme **involved approximately 1.15 million investors with an estimated loss of 38 billion renminbi (approximately S\$7.13 billion).**

During the investigations by PRC authorities into the Ponzi scheme, SPF uncovered more than S\$27 million of proceeds of crime that had been transferred to Singapore. SPF promptly alerted the PRC authorities. Subsequently, **in May 2016, SPF and the PRC MPS, with the assistance of the PRC Embassy in Singapore, conducted a joint investigation concurrently in China and Singapore. This collaboration led to the seizure of more than S\$27 million in Singapore.** SPF's investigations determined that no local entities were involved in money laundering activities related to the Ponzi scheme in Singapore.

Following the sentencing of 26 individuals involved in the Ponzi scheme by the Courts in China, **SPF repatriated the seized funds to China in August 2018. This facilitated the PRC government's restitution to the investors who were victims of the Ponzi scheme.**

#### **Box Story 15**

In January 2018, **SPF conducted an operation targeting individuals siphoning marine gas oil (MGO) from a petroleum refinery** on Pulau Bukom, an offshore island of Singapore. This action was prompted by credible information received on potential misappropriation of MGO.

During the operation, it was discovered that a **chemical-oil tanker, MT Prime South, had loaded approximately US\$962,000 (approximately S\$1.2 million) worth of stolen MGO.** The tanker was **seized as an instrument of crime** under Section 35 of the CPC. Subsequent investigations revealed that the MT Prime South was owned by Company A. Among those arrested were three employees of Company A.

**Within days of the operation, a Court order was obtained to return the stolen MGO, valued at US\$962,000 (approximately S\$1.2 million), to its rightful owner, the petroleum refinery.** This swift action aimed to minimise the degradation of the stolen MGO's quality due to exposure to the environment.

The three employees from Company A were **convicted and received imprisonment sentences ranging from 30 to 70 months. Additionally, cash totalling US\$50,000 (approximately S\$67,400) was confiscated from one of the employees, who held the position of Captain aboard the MT Prime South at the point of arrest.**

**MT Prime South was forfeited to the State** due to compelling evidence implicating the claimant in the offence, with the tanker being used in the commission of the crime at the time of the incident. MT Prime South was auctioned for US\$4.3 million (approximately S\$5.7 million) in June 2021, and the proceeds from the sale were forfeited to the State.



### 3.3 Loss Prevention

**3.3.1 Given the increasing prevalence of cyber-enabled crimes, particularly cyber-enabled fraud, Singapore seeks to reduce harm to innocent victims through loss prevention initiatives.** In Singapore, the total number of cyber-enabled fraud cases increased by 46.8% year-on-year to 46,563 in 2023, resulting in victims incurring losses totalling S\$651.8 million. Beyond financial losses, these cases can profoundly impact the lives of victims and their families, including psychologically.

**3.3.2 To achieve this objective, SPF established the Anti-Scam Command, facilitating the quick freezing and seizure of funds transacted through suspected criminal accounts.** Furthermore, the Anti-Scam Command instituted a 24/7 asset recovery mechanism with foreign counterparts to tackle cross-border transfer of criminal funds arising from cyber-enabled crimes and fraud (refer to **Box Stories 16 and 17**). Moreover, **staff from local banks and online platforms such as Carousell and Shopee, are co-located with SPF within the Anti-Scam Centre.** This collaborative arrangement has **enhanced synergy and expedited scam-related investigations** for law enforcement agencies.

#### Box Story 16

**SPF's Anti-Scam Command, together with the Hong Kong Police Force's Anti-Deception Coordination Centre (ADCC) and Singapore banks DBS and UOB, effectively thwarted a technical support scam, and successfully recovered more than S\$370,000.**

On 18 April 2024, DBS detected suspicious transactions totalling approximately S\$180,000 transferred from a 70-year-old victim's account to a bank account in Hong Kong. **The DBS Anti-Scam Team promptly intervened, halting further transactions from the victim's account to prevent further losses, and promptly alerted the Anti-Scam Command.** Leveraging this information, the **Anti-Scam Command swiftly notified the ADCC, highlighting the suspicious beneficiary account.**

The vigilance of the DBS Anti-Scam Team, coupled with the dedication of the Anti-Scam Command in exhausting all avenues to contact the victim resulted in swift action to safeguard the victim's savings. Upon learning from the victim's family friend that S\$240,000 was missing from the victim's UOB bank account, the **Anti-Scam Command promptly collaborated with UOB to suspend the victim's UOB bank account. Subsequently, they traced the funds to a bank account in Hong Kong.** Concurrently, working in tandem with the ADCC, they **successfully recovered the full amount** from the account in Hong Kong.

**The coordinated effort among DBS, UOB, ADCC and the Anti-Scam Command led to the successful recovery of more than S\$370,000 for the victim.**

### Box Story 17

**The Anti-Scam Command, in collaboration with six partnering banks - DBS, UOB, OCBC, HSBC, GXS, and Standard Chartered, is leveraging Robotic Process Automation (RPA) technology to identify victims of scams, including job, investment, and e-commerce scams. Employing a proactive approach, the Anti-Scam Command promptly alerts potential scam victims through Short Message Service (SMS) notifications, thereby mitigating the risk of further financial losses. Between 1 March and 30 April 2024, the Anti-Scam Command, in collaboration with partnering banks, sent out more than 16,700 SMS alerts to more than 12,500 scam victims who held accounts with these banks. This initiative led to the successful disruption of over 3,000 ongoing scams, preventing potential financial losses exceeding S\$100 million. Many of these victims only realised that they had fallen prey to scams after receiving the SMS alerts, which advised them to stop any further monetary transactions immediately.**

**3.3.3 The government proactively partners with private sector stakeholders to co-develop initiatives to tackle criminal activities.** For example, the Association of Banks in Singapore formed a Standing Committee on Fraud in 2022 to provide greater focus and coordination in the banking industry's anti-scam efforts. The committee comprises senior representatives from seven banks (DBS Bank, OCBC, UOB, Citibank, Maybank, Standard Chartered Bank, and HSBC) and collaborates with SPF and MAS to drive the banking industry's anti-scam efforts. The committee is currently focused on five workstreams: customer education, authentication, fraud surveillance, customer handling and recovery, and equitable loss sharing.

**3.3.4 At the industry level, the private sector has also proactively introduced loss prevention measures to stay ahead of criminals and protect their customers.** These measures include implementing anti-malware controls in mobile banking applications and introducing a "kill switch" to immediately freeze accounts and stop internet banking access when accounts are suspected to have been compromised. For example, banks have introduced a Money Lock feature in bank accounts, which customers can activate to lock and prevent a specified portion of their funds from being transferred digitally, in the event that their bank accounts are compromised (refer to **Box Story 18**).

### Box Story 18

Singapore's three local banks (DBS, OCBC, and UOB) have introduced a **Money Lock feature**, enabling customers to allocate a portion of funds in their accounts that cannot be transferred digitally. Once activated, the funds can only be withdrawn in person by the account holder at a branch or an Automated Teller Machine (ATM). This **limits the amount of funds a customer may lose** should his/her digital banking access be compromised.

Since its launch in November 2023 to February 2024, over **61,000 Money Lock accounts have been established, with savings exceeding S\$5.4 billion set aside through this initiative.** Other major retail banks in Singapore will progressively introduce the Money Lock feature by mid-2024.

### 3.4 Alternative Measures

#### 3.4.1 Singapore has expanded the suite of tools in our asset recovery regime to deprive criminals of their illicit proceeds.

- a) **Singapore has implemented civil measures targeting the proceeds of tax crimes.** IRAS is empowered with civil asset recovery powers under the Income Tax Act (ITA) and GST Act to claw back monies from criminals by imposing additional tax and financial penalties, which can amount to four times the sum of tax evaded and entail imprisonment terms of up to 10 years. IRAS enforces tax recovery through various measures, including the imposition of late payment penalties and the appointment of agents such as banks, employers, tenants, and lawyers (refer to **Box Story 19**).<sup>7</sup>

#### **Box Story 19**

In 2020, **Ng Cheow Chai (“Ng”)**, director of SMS Machinery (S) Pte Ltd (“SMS”) and precedent partner of Adept Machinery (“AM”), **faced 173 charges related to assisting 83 business entities (i.e. claimants) in submitting false information to the Comptroller of Income Tax to fraudulently obtain Productivity and Innovation Credit (PIC) cash payouts.**<sup>8</sup> Ng was also charged with one count of acquiring benefits from criminal conduct under the CDSA. **Ng received a 46-month imprisonment sentence and was ordered to pay a penalty exceeding S\$5.7 million to IRAS,** equal to four times the amount of the various payouts wrongfully obtained by the claimants, marking it as the **largest penalty and imprisonment term imposed for PIC fraud.**

IRAS referred the case to SPF for parallel financial investigations into possible ML offences. Investigations revealed that Ng instructed SMS’ staff to issue two quotations for each sale – one with the actual price and the other showing an inflated price. False invoices with inflated prices were provided to the PIC claimants for use in their PIC cash payout applications to IRAS. In some cases, no sales occurred between SMS and the PIC claimants. The PIC claimants paid SMS the inflated price stated in the false invoice, and SMS then refunded the difference between the inflated amount and the PIC cash payout amount to the PIC claimants via a false purchase from the PIC claimants by AM. Ng provided detailed instructions to create payment records indicating that the PIC claimants had made payments to SMS at the inflated price and to ensure that all payment records would be available if IRAS requested

<sup>7</sup> IRAS will appoint agents to recover the taxes owed by taxpayers if the taxpayers continually default on payment of their taxes. Any monies, funds, or other financial assets (such as bank accounts and salaries due from employers) belonging to the taxpayers and held by the appointed agents will be remitted to IRAS to settle the tax outstanding. The agents will be released from the appointment only after the taxes have been paid in full.

<sup>8</sup> Under the Productivity and Innovation Credit (PIC) scheme, businesses (sole proprietorships, partnerships, companies including registered business trusts, registered branches, and subsidiaries of a foreign parent or holding company) can enjoy 400% tax deductions / allowances for qualifying expenditure incurred in any of the six qualifying activities from Year of Assessment (YA) 2011 to 2018. For YA 2013 to 31 July 2016, eligible businesses can also exercise an irrevocable option to convert qualifying expenditure of up to S\$100,000 for each YA into cash, at a conversion rate of 60%. For qualifying expenditure incurred on or after 1 August 2016, the cash payout conversion rate has been reduced from 60% to 40%. The six qualifying activities are: (i) acquisition and leasing of PIC information technology and automation equipment; (ii) training of employees; (iii) acquisition and licensing of intellectual property rights; (iv) registration of patents, trademarks, designs, and plant varieties; (v) research and development; and (vi) investment in design projects.

supporting documents. This scheme effectively allowed the PIC claimants to obtain SMS machinery for free.

Through the course of the investigations and following Ng's conviction, IRAS had either **clawed back PIC cash payouts and bonuses** disbursed to claimants through IRAS' tax recovery powers or **disallowed PIC cash payouts and bonuses to claimants**.

- b) **Singapore has also employed voluntary restitution as a means to recover criminal proceeds.** This entails allowing offenders to voluntarily reimburse or compensate victims, thereby facilitating the recovery of illicit gains and mitigating the economic harm suffered by victims (refer to **Box Story 20**).

#### **Box Story 20**

In 2016, **Joanne Cheong Sook Yin ("Cheong")**, a product presentation manager at Nike, was sentenced to five months imprisonment for deceiving her employer by submitting false receipts amounting to approximately S\$77,000. Cheong **pleaded guilty to 22 charges related to the submission of inflated invoices**.

Between 2012 and 2014, Cheong submitted 154 inflated invoices from a company to **Nike**, resulting in the company paying out **S\$77,546 more than it should have**. **Cheong later made full restitution to Nike**.

## **Pillar 4: DETER criminals from using Singapore to hide, move, or enjoy their illicit assets**

### **4.1 Updated and Effective Legal Frameworks**

**4.1.1 Singapore constantly reviews and refreshes our laws to tackle emerging ML and criminal typologies.** Recent legislative amendments aim to bolster Singapore’s ability to combat ML upstream and enhance asset recovery and loss prevention measures.

- a) **CDSA Amendments in 2023** – introduced new provisions aimed at enhancing law enforcement agencies’ ability to combat ML. These changes empower authorities to take action against individuals acting as money mules in ML schemes and those assisting others in retaining proceeds from criminal activities and drug offences;
- b) **Online Criminal Harms Act in 2023** – grants SPF the authority to disrupt the recruitment of money mules by criminals for ML activities. This legislation allows SPF to direct online service providers to prevent suspected scam accounts or content from interacting with or reaching users in Singapore; and
- c) **Anti-Money Laundering and Other Matters Bill in 2024 (Upcoming)** – seeks to enable law enforcement agencies to launch ML investigations into foreign serious environmental crimes, such as illegal wildlife trading, illegal logging, waste trafficking, illegal land clearing, and illegal mining, which are rife in the Southeast Asian region.

#### Harsh Penalties and Sanctions

**4.1.2 Singapore implements stringent measures to deter ML within our financial system. Through severe penalties and sanctions, coupled with active publicity efforts via News Releases, we aim to raise awareness about the consequences of engaging in illicit financial activities.** By disseminating information about prosecutions and sentencing through various media channels, Singapore sends a clear message that such behaviour will not be tolerated (refer to **Box Stories 21 and 22**).

#### **Box Story 21**

In 2022, Juandi Pungot (“Juandi”), as part of a group conspiracy that misappropriated 203,403 tonnes of marine fuel valued at S\$128 million from his former employer, Shell Eastern Petroleum, received a sentence of **29 years’ imprisonment. This stands as one of the longest imprisonment terms ever imposed for a commercial crime.**

The sentencing took into account the **premeditated and sophisticated nature** of the offences, the **spectre of organised crime** raised by the syndicate, and the **transnational aspect** due to the involvement of foreign vessels.

Juandi’s sentencing included 7 to 10 years’ imprisonment for each Criminal Breach of Trust (CBT) charge, 11 to 20 months’ imprisonment for each ML charge, and 8 to 24 months’ imprisonment for each corruption charge. The Court ordered the sentences for the three CBT

charges, two ML charges, and a corruption charge to run consecutively, resulting in a total of 29 years' imprisonment, reflecting **Juandi's overall criminal behaviour**.

### **Box Story 22**

**On 2 August 2021, Rohaiza Alap, a 46-year-old Singaporean woman, received a sentence of seven years and four weeks' imprisonment for her involvement as a money mule, aiding overseas scammers in transferring more than S\$2 million out of Singapore.**

Rohaiza became entangled in ML activities through her boyfriend, a Nigerian man named Christian, whom she knew to be a scammer. Despite this knowledge, she began assisting him in his schemes in 2013, receiving funds derived from his scams into her bank accounts. Subsequently, Rohaiza transferred these sums to Christian, who compensated her with a commission of 5% of the criminal proceeds deposited into her accounts. Additionally, Rohaiza extended her assistance to other Nigerian scammers, earning a 10% commission for her services.

Over time, she opened multiple bank accounts, either under her own name or that of her company, to facilitate the receipt of criminal proceeds from the Nigerians. Furthermore, Rohaiza recruited seven others, including friends and relatives, to utilise their bank accounts for similar purposes.

Rohaiza pleaded guilty to 15 charges, including conspiring with others to receive criminal proceeds through their bank accounts, providing her bank accounts for the receipt of criminal proceeds, transferring cash exceeding the prescribed amount out of Singapore without reporting the movement, disclosing prejudicial information, and intentionally aiding someone in possessing money reasonably suspected of being stolen or obtained fraudulently.

## **4.2 Public Education and Partnerships**

**4.2.1 Recognising that the public is the first line of defence against ML and criminal activities, Singapore adopts a whole-of-society approach towards crime-prevention and asset recovery.** As part of this strategy, Singapore has launched an extensive public education campaign aimed at safeguarding individuals from becoming victims of crime. With the surge in cyber-enabled fraud and ML cases in recent years, particular attention is given to emerging ML and criminal typologies, notably those involving money mules.

- a) **Through collaborative efforts with the private sector and the community, the government has been mobilising banks and community stakeholders to take a proactive stance against ML and criminal activities.** In recent years, a robust partnership has been forged between the government and banks to bolster community vigilance against cyber-enabled fraud and safeguard the financial interests of customers (refer to **Box Story 23**).

### Box Story 23

Between February and March 2024, an 82-year-old man experienced **three attempts by scammers to defraud him, amounting to a potential loss of S\$3.7 million.** However, due to the swift intervention of the Anti-Scam Command, CIMB Bank, and Hong Leong Finance, these attempts were thwarted.

On 6 February 2024, CIMB's fraud management team detected transactions amounting to S\$2.1 million made from the victim's bank account. Responding promptly, the Anti-Scam Command and CIMB officers visited the elderly victim at his home. While **CIMB's fraud management team suspended the victim's bank account to prevent further losses,** the Anti-Scam Command provided support to the victim through his son. **Although S\$1.3 million was recovered,** the remainder had already been transferred overseas before the police report was made.

On 7 February 2024, the victim's son alerted the Anti-Scam Command about three cheques amounting to S\$1.2 million issued by Hong Leong Finance under the victim's instruction to three individuals. The Anti-Scam Command promptly requested Hong Leong Finance to withhold the cheques, **averting a potential loss of S\$1.2 million.**

On 9 March 2024, the scammers attempted another scheme, accompanying the victim to CIMB's branch office to purchase a cashier's order of S\$1.2 million. The vigilant CIMB team promptly alerted SPF, leading to the arrest of the scammers. This **further prevented the loss of S\$1.2 million.**

The close collaboration between SPF and the banks, combined with quick action **to engage the victim and suspend transactions, proved instrumental in** preventing the loss of S\$3.7 million. The **vigilance of the victim's son and CIMB officers** was crucial in **detecting suspicious transactions,** contributing to the minimisation of financial losses and the resolution of the situation.

- b) **SPF conducts public education events to raise awareness among youths on the repercussions of engaging in criminal activities, particularly becoming a money mule.** One such event, the *Criminal Behavioural Analysis Competition 2023: Youths Against Scams* held in July 2023, served as a platform to engage and educate youths on the preventive actions they can take to protect themselves from falling prey to scams, and were provided valuable insights on how to protect themselves from falling victim to fraudulent schemes (refer to **Box Story 24**).

### Box Story 24

**The Delta League programme, initiated in 2011, is a biannual youth engagement programme** jointly organised by SPF and the National Crime Prevention Council (NCPC) to engage youths in sports and crime prevention activities. **In 2023, over 1,200 youths participated** in activities aimed at educating them about scams and how to avoid being unwittingly involved as money mules.

#### 4.2.2 Recognising the important role members of the public play in combatting criminal activities, law enforcement agencies actively partner the public in detecting suspicious activities through anonymous whistleblowing mechanisms.

- a) To encourage the **reporting of malpractices, IRAS provides an informant reward for valuable information leading to tax recovery.** This reward amounts to 15% of the tax recovered, with a cap of S\$100,000, to be granted to informants if the provided information and/or documents results in the recovery of tax that would have otherwise been lost. Informants can report instances of tax evasion through an online reporting template available on IRAS' website.
- b) To enhance the **detection of corruption**, CPIB has implemented various reporting channels, including the **CPIB Duty Officer hotline** and lodging an **e-Complaint for Corrupt Conduct**.
- c) To strengthen Singapore's overall AML/CFT regime, all individuals, including FIs and DNFBPs, are **legally obligated to file STRs to STRO** if they know or have reasonable grounds to suspect that any property is linked or intended to be used in connection with a criminal activity. Additionally, sectoral regulators actively engage with their supervised sector on trends and typologies identified based on the information received in the STRs. They also conduct AML/CFT inspections and take appropriate enforcement actions in cases of non-compliance with AML/CFT requirements by the supervised entities. STRO also disseminates red flag indicators to law enforcement agencies and industry partners to improve the detection of ML activities and increase the likelihood of asset recovery.



## CONCLUSION

1. **ML and criminal threats are constantly evolving, resulting in increasing socio-economic harm to society.** The scale and complexity of ML and criminal threats have increased with substantial sums of money being laundered by criminals, often across borders. To safeguard Singapore's financial system, every effort will be made to **detect** abuse and **deprive** criminals of their ill-gotten gains, while remaining a welcoming environment to legitimate businesses. These are mutually reinforcing objectives that strengthen confidence of both international businesses and the public in the Singapore system.
2. **Maximising asset recovery is crucial for providing restitution to victims.** We seek to **deliver** maximum restitution to victims and affected parties through active cooperation with foreign counterparts and industry partners. Additionally, we leverage innovative technology to support asset recovery efforts in the face of increasingly sophisticated ML and criminal activities. These initiatives will further bolster Singapore's reputation as a trusted international financial centre and business hub.
3. **Asset recovery requires a whole-of-society approach.** Singapore will continue to actively partner the public in combatting criminal and ML activities, and be steadfast in our resolute and decisive measures to **deter** criminals from exploiting Singapore's ecosystem. We will continuously refine our asset recovery strategy in the face of evolving criminal and ML threats.