

INTER-MINISTERIAL COMMITTEE ON ANTI-MONEY LAUNDERING



CONTENTS



FOREWORD BY
IMC CHAIRPERSON | 03

EXECUTIVE
SUMMARY | 05

INTRODUCTION | 07

PROACTIVE
PREVENTION | 13

TIMELY DETECTION | 23

EFFECTIVE
ENFORCEMENT | 31

CONCLUSION | 38

FOREWORD

Indraneel Rajah

Minister in the Prime
Minister's Office

Second Minister for
Finance and National
Development

Chair of the Inter-
Ministerial Committee
on Money Laundering



Trust is the cornerstone of a sound financial centre and business hub. It provides individuals and businesses with the confidence to conduct their activities. At the same time, this trust can also be undermined by criminals seeking a safe haven for their illicit assets.

Over the years, Singapore has painstakingly built a strong foundation of trust, marked by our strong stance against money laundering, readiness to act against criminals, and commitment to continuously improve our regulatory framework.

As a society, we have stayed true to these principles, as seen from our decisive action in the major money laundering case in August 2023. The intelligence gathered from various sources, including suspicious transaction reports filed by financial institutions and other gatekeepers, enabled our law enforcement agencies to bring the criminals to justice.

The case highlighted valuable lessons on how criminals have adapted their tactics to evade our safeguards. Hence, we established the Inter-Ministerial Committee to review our anti-money laundering framework to ensure that our system remains relevant against increasingly sophisticated criminal

tactics. The Committee's recommendations and accompanying measures are detailed in this report, except for those with operational sensitivities. In this constant game of cat-and-mouse, we must avoid revealing information that would help potential bad actors circumvent our defences.

The Committee's work has benefitted from the support of many stakeholders – from industry bodies and professionals, to law enforcement and regulatory agencies. I thank everyone who generously contributed their insights, and am encouraged by the increased societal awareness of money laundering.

The Committee has calibrated its recommendations to further strengthen our framework against money laundering, so that we do not place undue burden on the large majority of businesses, which are legitimate. We continue to welcome legitimate investors and businesses, while remaining watchful and not falling prey to the allure of dirty money, to avoid tarnishing our hard-earned reputation as a trusted business hub.

The Government is already implementing these recommendations, and I am certain that gatekeepers will similarly step up their vigilance. However, the reality is that there is no silver bullet to completely eradicate

money laundering. At some point in the future, some bad actors will find new ways of laundering their illicit wealth, and some gatekeepers will be unable to say no to its allure. That is all it takes for criminals to enter our system. When this happens, we will take decisive action against them.

Strengthening our defences against money laundering is an ongoing effort that requires

more than just government action. Everyone has a role to play to stay vigilant to suspicious activities. Gatekeepers like financial institutions, real estate salespersons, and precious stones and precious metals dealers must continuously watch out for suspicious activities when dealing with clients. Ordinary citizens can also do their part by reporting suspicious individuals, businesses or property to the Police.

We must collectively stand firm against criminals and their dirty money. Only then can Singapore remain an attractive, dynamic and trusted financial centre - welcoming to legitimate investors and businesses, while staying resolute in our actions against criminals and their illicit assets.

EXECUTIVE SUMMARY

Money laundering is a serious crime that undermines the integrity of financial systems. As a reputable and trusted financial centre and business hub, Singapore takes a robust stance against money laundering, while being welcoming and facilitative towards legitimate businesses.

We have a strong legal and institutional framework against money laundering.

As a result, the Singapore Police Force (SPF) was able to detect, track and execute one of the world's largest crackdowns on money laundering in August 2023. More than \$3 billion in assets were seized or issued with prohibition of disposal orders, and ten persons have been arrested and convicted.

To further strengthen our system, the Inter-Ministerial Committee (IMC) was set up in November 2023 to review Singapore's anti-money laundering (AML) framework with the benefit of experience gained from this money laundering case.

The IMC is chaired by Minister Indranee Rajah, Minister in the Prime Minister's Office and Second Minister for Finance and National Development, and comprises Political Office Holders and representatives across the Government.

This report sets out the IMC's review and recommendations. We adopt a whole-of-society approach, where relevant stakeholders are part of our frontline of defence and work collaboratively with relevant government agencies.

The IMC is strengthening the three key pillars of Singapore's AML framework:

- 1 Prevent
- 2 Detect
- 3 Enforce

INTRODUCTION



What is money laundering?

Money laundering is the process of making criminal proceeds appear legitimate to evade detection, by disguising their illegal origins. Criminals do this by hiding the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Money laundering is a complex crime that spans different jurisdictions. The proceeds being laundered could come from various criminal activities, like fraud, organised crime, corruption or tax crimes.

Each party – from sector supervisors, law enforcement agencies, and gatekeepers – must do their part to combat money laundering. For instance, money laundering can still occur despite stringent regulations, if gatekeepers flout these regulations. Supervisors and law enforcement agencies must then be resolute in taking the necessary enforcement action against the gatekeepers and criminals respectively, to take them to task and deter others from committing such offences.

If it is not dealt with, money laundering can severely undermine the integrity of financial systems, impeding economic growth and deterring investments and business activities. We must therefore take decisive action against money laundering and prevent overseas crime syndicates from laundering their illicit assets to fuel their criminal activities.

Today, Singapore is a destination of choice for companies and individuals to do business and invest their wealth. Singapore's success as an international financial and business hub stems from our political and economic stability, strong rule of law, and pro-business policies and regulations.

Singapore is committed to preserving our trusted and conducive business environment. This is why Singapore has established an AML framework that is robust, yet balanced, to deter bad actors from exploiting our economic openness to launder illicit funds, while providing ample opportunities for legitimate businesses to thrive and grow.

Singapore's AML efforts are led by the Anti-Money Laundering/Countering the Financing of Terrorism Steering Committee (AML/CFT SC), comprising the Permanent Secretaries of the Ministry of Home Affairs (MHA) and Ministry of Finance (MOF), and the Managing Director of the Monetary Authority of Singapore (MAS). The SC oversees Singapore's AML efforts and ensures coordinated action across government agencies to combat money laundering. The Government also works closely with industry partners and gatekeepers.

PROACTIVE PREVENTION



We will build on our existing frameworks to **proactively prevent** criminals from laundering their illicit proceeds.

- 1 **Strengthen anti-money laundering standards** for gatekeepers
- 2 **Further support gatekeepers** to enhance capabilities to combat money laundering
- 3 **Engage non-regulated sectors** to enhance their understanding of money laundering risks
- 4 **Strengthen mechanisms** to deter misuse of companies

TIMELY DETECTION



We will enable sector supervisors and gatekeepers in the **timely detection** of illicit activities.

- 1 **Strengthen sensemaking and information sharing within government**
- 2 **Deepen channels for data sharing** amongst and with gatekeepers

EFFECTIVE ENFORCEMENT

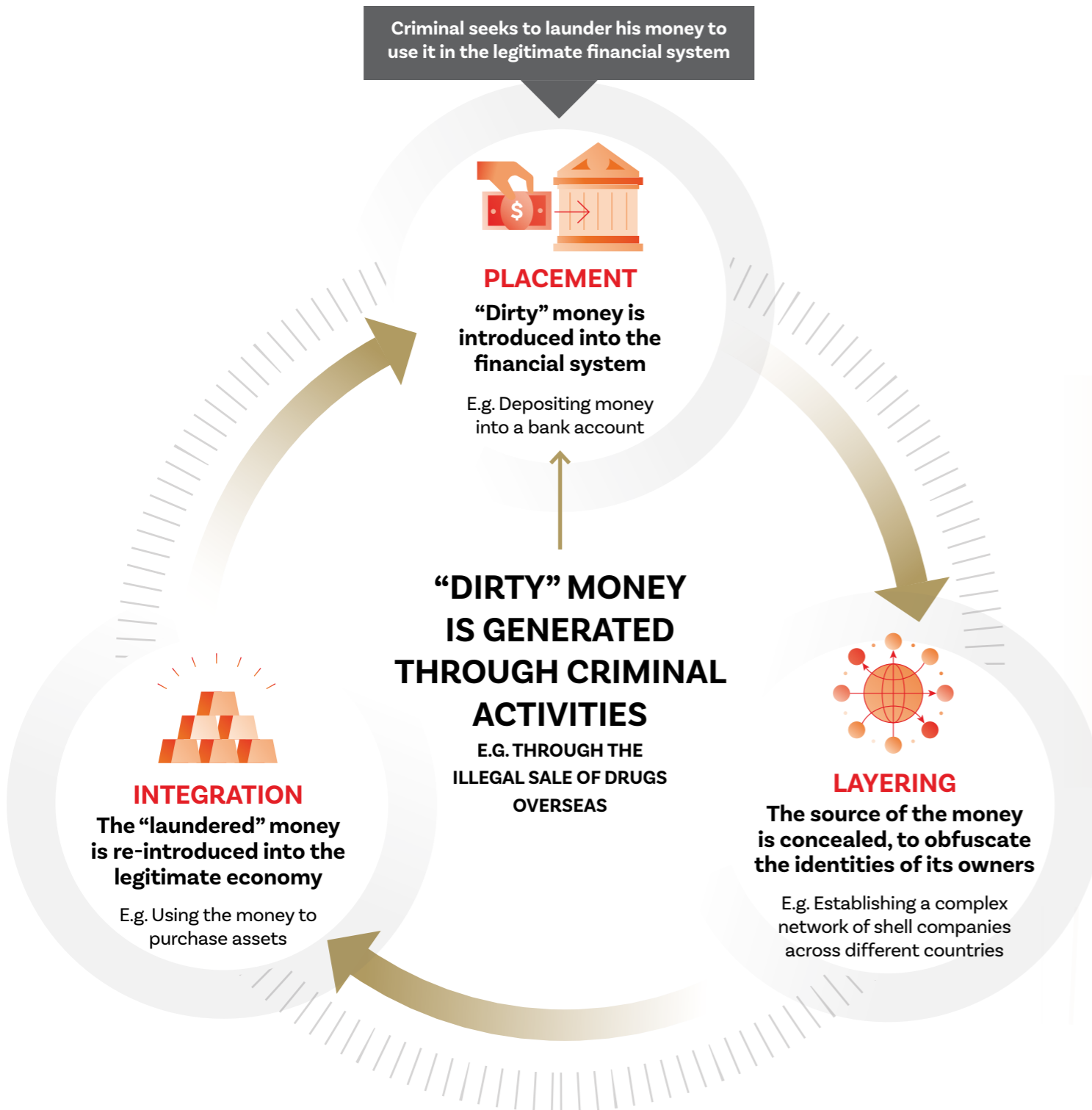


We will take **effective enforcement** actions against criminals who engage in illicit activities.

- 1 **Enhance legislative levers** for law enforcement agencies to better pursue and prosecute money laundering offences
- 2 **Continuously review penalty frameworks** to ensure they remain proportionate and dissuasive
- 3 **Strengthen inter-agency coordination** to enable swifter and more effective action against illicit money laundering activities

It is crucial to be pragmatic and recognise that no society will be able to completely eradicate money laundering. The IMC's recommendations seek to reduce its likelihood and strengthen our actions in dealing with such cases.

WHAT IS MONEY LAUNDERING?



This is a simplified example. Real world cases can be far more complex, with multiple actors and iterations involved at each stage, and with back and forth between the various stages for further obfuscation.

Combatting money laundering is a whole-of-society approach, because it requires all stakeholders in the ecosystem to fulfil their roles:

- Legislation lays the foundation for these efforts. It criminalises money laundering, and prescribes gatekeepers’ obligations to combat money laundering and the sanctions that apply. However, legislation alone cannot completely prevent money laundering. It can deter such crimes, but it will not eliminate it altogether.
- This is why gatekeepers have a significant role to play in combatting money laundering. They serve clients and must be vigilant against the misuse of their services. Gatekeepers must comply with their obligations, or face sanctions. Such sanctions also seek to dissuade gatekeepers from neglecting their obligations.
- Legislation also cannot eliminate human error, negligence and fraud. While most gatekeepers are responsible and compliant, a minority will inevitably be tempted by the allure of dirty money and turn a blind eye to money launderers.
- When this occurs, law enforcement authorities and sector supervisors must take the appropriate measures against criminals and gatekeepers respectively and hold them responsible for their misdeeds.

Therefore, Singapore’s AML framework is underpinned by a three-pronged strategy - **Prevent, Detect and Enforce**:

First, strengthening our legal and regulatory framework to **Prevent** criminals from operating in Singapore;

Second, developing measures to better **Detect** signs of illicit activity; and

Third, taking decisive administrative, regulatory and criminal measures to **Enforce** our laws.

Singapore continually updates our defences against money laundering to deal with emerging risks and threats. We ensure that our policies and levers remain up to date with international standards set by the Financial Action Task Force (FATF), tailored to our domestic risks.



The FATF leads global action to tackle money laundering, terrorist and proliferation financing. Established in 1989, the FATF sets international standards aimed at preventing these illicit activities and promotes the effective implementation of legal, regulatory and operational measures for combatting threats to the integrity of the international financial system. Over 200 countries and jurisdictions have committed to implement the FATF Standards.

In the last Mutual Evaluation of Singapore in 2016, the FATF assessed Singapore to have a strong legal and institutional framework to fight money laundering and terrorism financing, with sophisticated and comprehensive coordination efforts, involving all the relevant authorities across the public and private sectors.

Singapore's next Mutual Evaluation will take place in 2025, and Singapore is determined to maintain our good standing.

Many qualities that make Singapore appealing to businesses and investors are also attractive to money launderers. Regardless of how robust our AML framework is, these criminals will still attempt to circumvent our defences. Depending on the sophistication of the methods that criminals use, and the vigilance of financial institutions and other gatekeepers, some money laundering activities may remain undetected. This is not unique to Singapore - all international financial centres are vulnerable to bad actors.

At the same time, we must strike an appropriate balance when calibrating our AML defences. If our measures are too lax, bad actors will take advantage and compromise the integrity of our system. If we are overly-restrictive, it may unduly hinder legitimate businesses, resulting in opportunity costs for our economy and our people.

This is why in exercising our three-pronged strategy against money laundering, we constantly strive to maintain this balance. Our measures to Prevent, Detect and Enforce against money laundering seek to create a reinforcing loop to deter and stamp out bad actors, while allowing legitimate firms to thrive within a pro-business regulatory environment.

The decisive actions we took to uncover the recent money laundering case and bring the criminals to justice demonstrate Singapore's commitment to combat money laundering. The Police took a comprehensive approach in rooting out the syndicate, drawing information from multiple sources, including Suspicious Transaction Reports (STRs). Ten individuals have been arrested and dealt with, including imprisonment and forfeiture of over 90 percent of their seized assets.



Key Facts

KEY FACTS OF AUGUST 2023 MONEY LAUNDERING CASE

In early 2022, Police launched a comprehensive, coordinated intelligence probe, which discovered a web of individuals believed to have various connections amongst themselves, and significant assets held by these individuals in Singapore. This probe was conducted covertly, to avoid alerting the suspects.

Prior to this, elements of the case had 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, filed by financial institutions and other companies.

By August 2023, Police had gathered sufficient evidence to take action. On 15 August 2023, ten suspects were arrested in a series of simultaneous raids at multiple locations across Singapore. Generally, they were found to have:

- Registered companies, both foreign and local, under their names
- Utilised the companies, by securing work passes to legitimise their stay and opening bank accounts to funnel their illicit funds
- Utilised the illicit funds to purchase properties and precious products, such as gold bars, luxury watches and jewellery

More than \$3 billion of suspected illicit financial and physical assets, including cash, cryptocurrencies and luxury goods were seized or prohibited from disposal in this AML operation, one of the largest undertaken globally.

As of July 2024, all ten subjects have been convicted of money laundering and other offences, and sentenced to imprisonment of between 13 and 17 months for the offences that they had committed in Singapore. More than 90% of the properties seized from these individuals, totalling approximately more than \$940 million, have been forfeited to the State. All ten subjects have been deported after serving their sentence and barred from re-entering Singapore.

In addition, investigations are ongoing against 17 persons who are not in Singapore, involving approximately \$2 billion of seized assets.

Following the recent money laundering case, we established the IMC in November 2023 to review Singapore's AML framework and ensure it remains up to date against increasingly sophisticated crimes.



The IMC's review focused on five key areas:

- How to better prevent money launderers from misusing corporate structures;
- How financial institutions can enhance their controls and collaborate more effectively with one another and the authorities to identify and flag suspicious transactions;
- How other gatekeepers in the system, like corporate service providers, real estate salespersons and estate agencies, and precious stones and precious metals dealers can better guard against money laundering risks, including the adequacy of the existing regulatory framework over these players;
- How to better centralise and strengthen monitoring and sense-making capabilities across government agencies to detect suspicious activities; and
- How to strengthen enforcement levers and capabilities to enable firm and decisive actions against money launderers, including depriving them of ill-gotten proceeds.

The IMC's recommendations aim to strengthen Singapore's three-pronged AML strategy – Prevention, Detection and Enforcement – and are supported by accompanying measures. The IMC also reviewed measures that were already being developed before the case, and which can benefit from relevant insights from the case.

The IMC has calibrated its recommendations to enhance our effectiveness in combatting money laundering, without placing undue burden on the vast majority of businesses that are legitimate. Given the constantly evolving nature of criminal typologies, we may not eradicate money laundering cases altogether. But these recommendations reduce the likelihood of money laundering and strengthen the actions we take in dealing with such cases, as and when they happen.

PROACTIVE PREVENTION

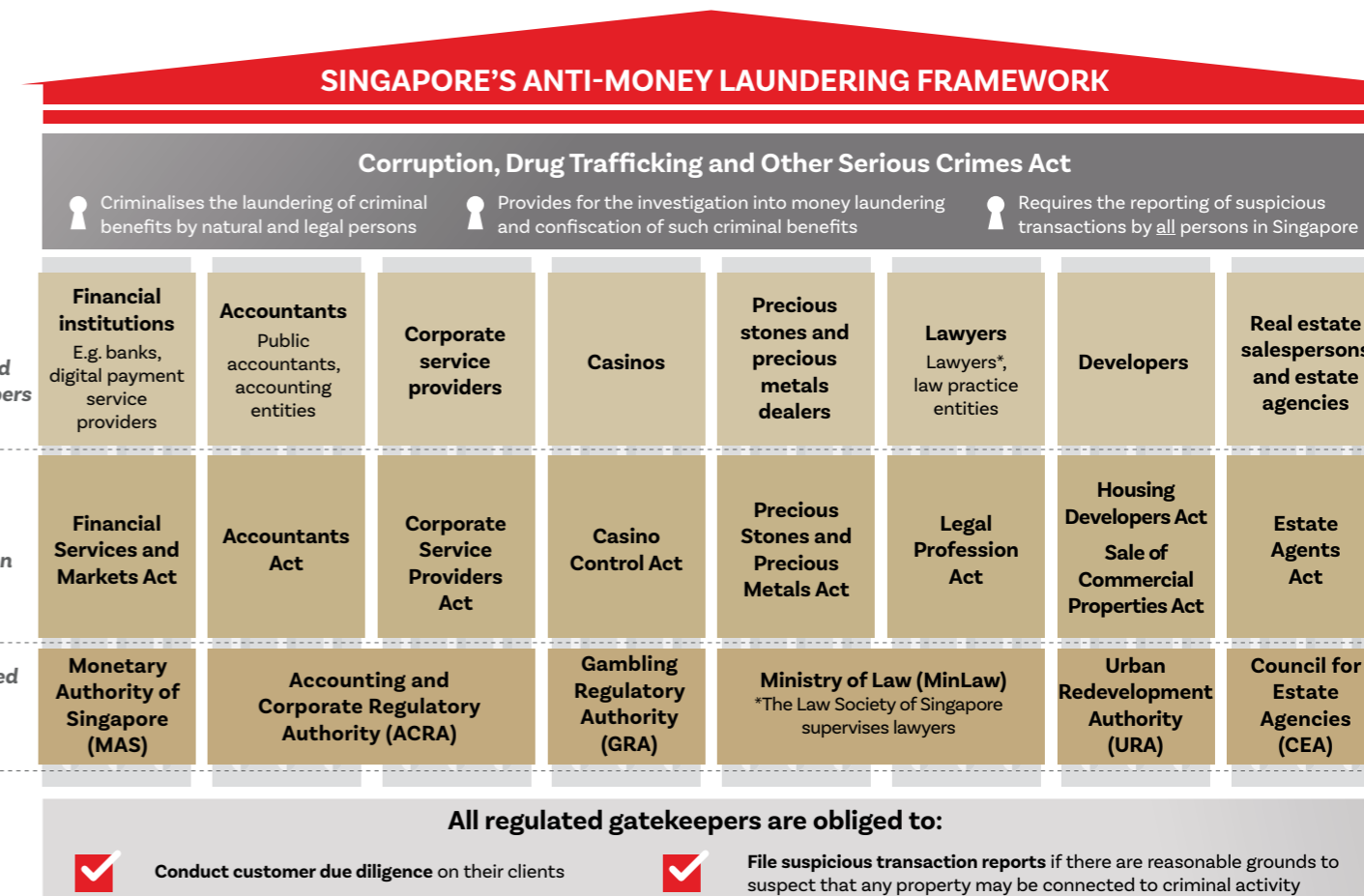


Prevention is the first prong of Singapore's strategy against money laundering. We can prevent criminals from laundering their illicit proceeds in Singapore by turning away bad actors and illicit transactions in the first instance.

Prevention relies primarily on "gatekeepers" in the private sector, especially financial institutions and designated non-financial businesses and professions (DNFBPs)¹. Gatekeepers are usually the first touchpoints for new businesses or individuals setting up in Singapore. They should have a good

understanding of the behaviours that would be considered normal, unusual or suspicious within their industry. This makes them well-positioned to assess the risk of clients misusing their services for criminal purposes.

Gatekeepers must comply with the AML requirements set by their sector supervisors. These requirements guide gatekeepers' conduct, by imposing legal obligations on them to perform their duties. Gatekeepers that do not comply face serious consequences, such as fines, convictions and the cancellation of their professional registrations.



Sector-specific obligations and supervisory expectations are further detailed in legislation and guidance, calibrated according to sectoral risks

¹ Under the FATF's standards, Designated Non-Financial Businesses and Professions are defined as (i) casinos, (ii) real estate salespersons and estate agencies, (iii) dealers in precious metals, (iv) dealers in precious stones (v) lawyers, notaries, other independent legal professional, (vi) accountants and (vii) Trust and Company Service Providers.

Singapore adopts a risk-based AML approach. The foundational requirements are aligned across gatekeepers, with adjustments to account for differing risks and contexts of each sector. The key obligations of gatekeepers include:


- **Conducting customer due diligence (CDD)** before starting a relationship with a new customer, at a level commensurate with the customer's risk profile.
- **Filing a suspicious transaction report (STR)** promptly upon detecting any suspicious activities during interactions with customers.

Gatekeepers should also conduct ongoing monitoring of their business relationships with clients (such as ensuring that documents are kept up-to-date), calibrated based on the risk of clients' transactions and profiles.

An effective AML framework requires the collective effort of all gatekeepers. No single gatekeeper has sight of the entire web of illicit activities, as criminals can carry out their misdeeds across a broad range of industries, products and services. Criminals may abuse the services of multiple gatekeepers to "place" their illicit proceeds in Singapore, "layer" or disguise their origin, and then "integrate" these laundered proceeds into the legitimate economy.

Notwithstanding existing AML controls, we observed uneven implementation practices across and within sectors. If gatekeepers do not do what they are expected to do despite Singapore's robust AML regulations, it will be difficult to combat money laundering. We must thus strengthen the execution of these controls, and sector supervisors must provide more comprehensive guidance to gatekeepers.

Some measures to strengthen our Prevention capabilities were underway before the recent case was surfaced. **We reviewed relevant measures already under development and also recommend new measures, to Proactively Prevent criminals from laundering their illicit proceeds.**

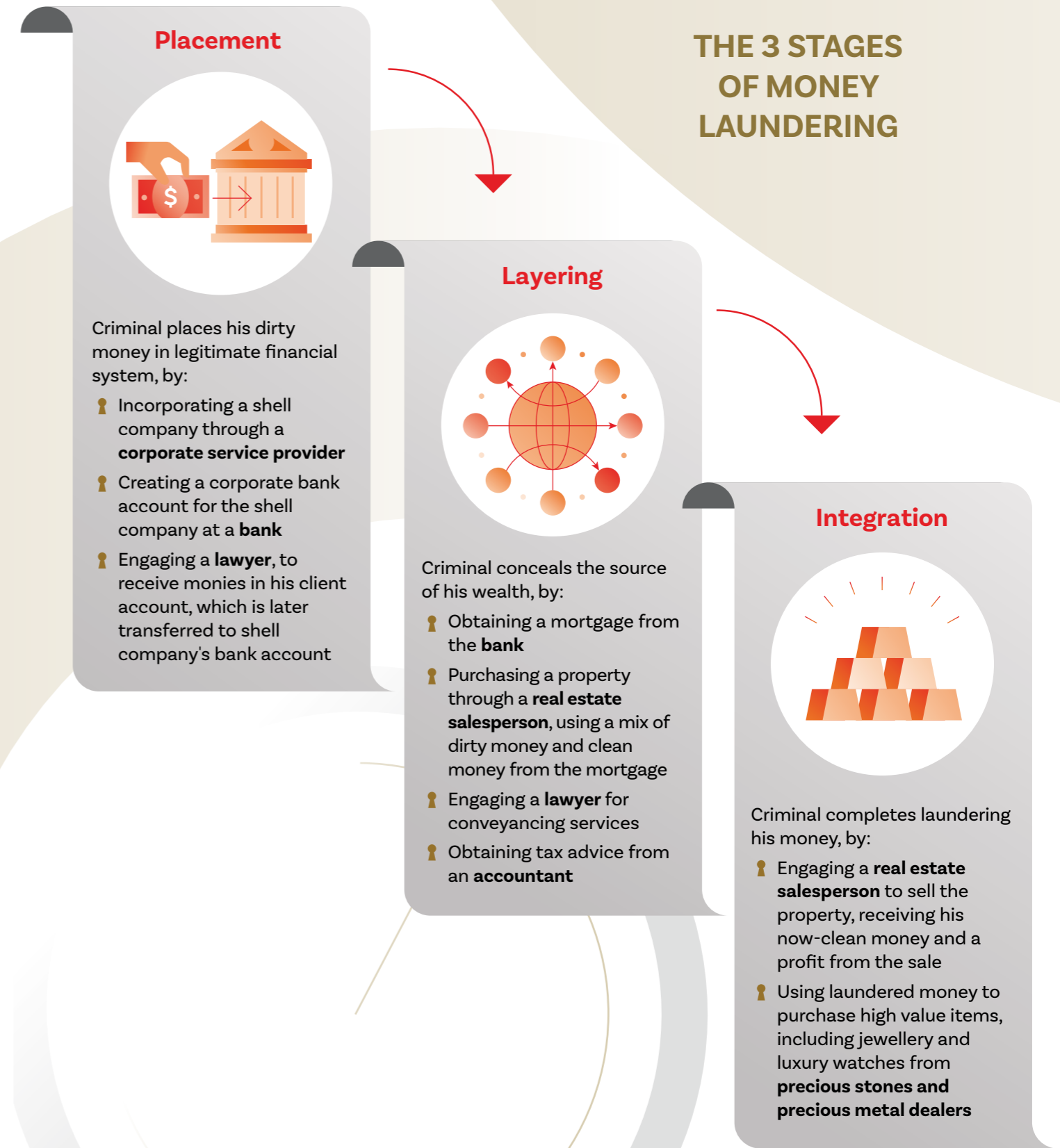


What are Suspicious Transaction Reports (STRs)?

STRs form financial intelligence that is essential in the detection of money laundering, terrorism financing and other serious crimes. An STR is a report that everyone must file with the Suspicious Transaction Reporting Office (STRO), if there are reasonable grounds to suspect that any property may be connected to drug dealing or criminal conduct, through the course of their trade, profession, business or employment. An STR must be filed to disclose the knowledge or suspicion as soon as is reasonably practicable.

The reporting requirement is set out in Section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA).

THE 3 STAGES OF MONEY LAUNDERING



REVIEW & RECOMMENDATIONS



1 Strengthen AML standards for gatekeepers

To ensure a consistent baseline in AML standards and prevent criminals from exploiting any weak link, sector supervisors are strengthening their existing AML/CFT frameworks to address emerging risks.

Precious stones and precious metal dealers (PSMDs) to conduct CDD on a broader range of products

PSMDs are regulated under the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019 (PSPM Act). “Precious products” were previously defined as any jewellery, watch, apparel, accessory, ornament or other finished products, with at least 50% of their value attributable to PSPM. This definition excluded precious products whose value was largely attributed to other factors besides PSPM, such as branding or workmanship, even if they were of a high value.

In February 2024, the PSPM Act was amended to expand the scope of precious products, to include PSPM products priced above \$20,000, regardless of the value attributable to the PSPM components.

Consequently, PSMDs are now required to conduct CDD and file cash transaction reports on transactions involving a broader range of precious products.

Lower threshold for casino operators to conduct CDD checks

Casino operators are regulated under the Casino Control Act. In August 2024, the Casino Control Act was amended to reduce the threshold for CDD checks, from the previous threshold of \$10,000 for single cash transactions and \$5,000 in deposits, to \$4,000 for both single cash transactions and deposits.

Consequently, casino operators are now required to conduct CDD on more transactions, to better prevent criminals from using casinos as an avenue for laundering their proceeds.

Upcoming clarifications for real estate and legal sectors

We will also clarify the requirements for real estate salespersons, estate agencies, developers, lawyers and law practice entities to conduct CDD and ongoing monitoring of their clients. There are already existing CDD requirements under the respective sectoral regulations², which are aligned with international standards. We make clear that the gatekeepers need to identify and take reasonable measures to verify the identities of the individuals³ that their clients may be acting on behalf of. This is because the clients interacting with these gatekeepers might not be the ultimate beneficial owner of a transaction or asset, which could lead to potential risks of abuse.

² These are the Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations, Housing Developers (Anti-Money Laundering and Terrorism Financing) Rules 2023, Sale of Commercial Properties (Anti-Money Laundering and Terrorism Financing) Rules 2023, and Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015 respectively.

³ In addition to identifying and verifying the identities of the ultimate beneficial owners of businesses, which is already required.

Overall, all sector supervisors will continue to review and monitor gatekeepers' compliance with the AML obligations. This will increase the overall baseline consistency in AML practices.

2 Further support gatekeepers to enhance capabilities to combat money laundering

Gatekeepers must be equipped to fulfil their AML responsibilities effectively to complement the enhanced AML requirements. While we have robust AML requirements, we observed that gatekeepers' practices vary and fall short in some instances. **Sector supervisors will provide more guidance on AML practices to set a clearer baseline for their respective sectors.** For sectors where the AML obligations are more nascent, sector supervisors will work with gatekeepers to improve their capabilities.

Sector supervisors to provide more guidance on AML practices

Gatekeepers must conduct CDD and take appropriate mitigating measures when dealing with higher-risk or suspicious clients. These include:

- **Client risk assessments** to gauge the level and nature of the client's risk. Gatekeepers must apply mitigating measures, such as enhanced due diligence, for clients assessed to pose a higher risk.
- **Identifying source of wealth or funds** that the client intends to use for

transactions or deposit into a bank account, in cases where there are higher ML risks. To assess the legitimacy of client assets, gatekeepers must understand how they are derived. Gatekeepers must ask the right questions to evaluate the legitimacy of a client's source of wealth or funds, and obtain adequate information to support their assessment.

- **Filing STRs in a timely manner**, if gatekeepers have reasonable grounds to suspect illicit activity or that they have illicit origins, when interacting with their customers.

Sector supervisors will provide more guidance on AML practices in the coming months, to clarify supervisory expectations and better equip gatekeepers. The guidance will broadly follow the same principles, tailored to the different sectors. For example, these principles for source of wealth (SOW) and source of fund (SOF) checks will be set out in the updated guidance:

- Gatekeepers should obtain corroborative evidence or conduct independent checks (i.e. not rely solely on the client's declaration).
- Gatekeepers should make a reasonable assessment on the plausibility of clients' SOW, with proper documentation of the assessments.
- The extent of checks and corroboration should be guided by a risk-based approach, and not unduly hinder legitimate businesses and individuals.

Sector supervisors to engage gatekeepers closely and enhance gatekeepers' training

To complement the additional AML guidance, supervisors will also further equip gatekeepers through engagements and enhancements to training.

Sector supervisors already engage their respective sectors through industry events and guidance. Supervisors will continue using these platforms and develop additional ones if needed, to share their observations on changing AML risks and typologies. These efforts will raise awareness on evolving risks, and enable gatekeepers to discharge their duties more effectively.

Proper training is critical to equip gatekeepers with the capability to identify high risk circumstances and take appropriate actions, including filing STRs in a timely manner. Such training is administered by professional bodies and course providers, which gatekeepers are highly encouraged to attend.

Sector supervisors will enhance the quality and accessibility of training. For example, CEA will mandate AML courses and work with course providers to raise the quality of training. CEA will also explore if such training courses can be paid using SkillsFuture credits.

Gatekeepers should proactively stay updated with latest developments and requirements, and attend relevant courses.

3 Engage non-regulated sectors to enhance their understanding of ML risks

Criminals may use their ill-gotten proceeds to buy high-value goods, whether for personal enjoyment or to re-sell them and further obfuscate the illicit origin of their wealth.

Nevertheless, applying AML requirements to all high-value goods dealers would be impractical, as it would significantly burden legitimate businesses and consumers, without clear benefits to the authorities.

We adopt a risk-based approach in line with the FATF's international standards, focusing on higher-risk areas identified to be more vulnerable to money laundering, such as high-value items that contain PSPM.

This does not mean that unregulated sectors, including dealers of high-value goods other than PSPM, have no AML obligations at all. **Under the CDSA, anyone who knows, or has reasonable grounds to suspect that any property may be connected to criminal conduct through the course of his trade, profession, business or employment, must file an STR to disclose the knowledge or suspicion as soon as is reasonably practicable. Those who fail to do so may be committing an offence that attracts sanctions. Everyone has a role in preventing money laundering.**

Education efforts for high-value goods dealers on money laundering risks and their obligations

To increase the understanding of risks across the ecosystem, we will engage high-value goods dealers who are currently unregulated, to raise their awareness of money laundering risks. We will also highlight how they can mitigate these risks (such as not accepting large payments in physical cash), and educate them on how to file an STR. This will make it harder for criminals to transact with these dealers, without placing undue restrictions on legitimate activities.

We will also continue to monitor if specific goods should be regulated or supervised more closely.

4 Strengthen mechanisms to deter misuse of companies

Companies are crucial in enabling and supporting business activities. Incorporating a company in Singapore is generally straightforward and streamlined. Companies and the individuals controlling them, such as their directors, are subject to legislative requirements under the Companies Act. However, companies can be misused by criminals for illicit purposes.



Two ways in which companies can be misused for money laundering are through shell companies and front companies.

1. A **shell company** is a company with no ongoing operations, business activities or significant assets.
 - All companies start as shell companies in their first phase of incorporation. Many eventually become fully operational and carry out legitimate business activities. Others may remain as shell companies for legitimate purposes, such as transaction vehicles for corporate mergers, or for international companies that have not established operations in Singapore, to protect their names from being used by others.
 - However, criminals may also launder their illicit proceeds through the misuse of shell companies, such as by disguising their beneficial ownership through complex structures and facilitating the movement of funds by using corporate bank accounts set up in the name of these shell companies.
2. A **front company** is a company that is seemingly legitimate through its business operations, but is in practice conducting illicit activities.
 - Criminals can channel their illicit proceeds, disguised as legitimate sales revenue, through these front companies. The idea is to "clean" the dirty money by mixing it with legitimate income, making it difficult to trace the original source.
 - One method used in the past is through laundromats which are predominantly cash-based businesses, hence the origin of the term "money laundering". Today, money laundering has gone beyond laundromats, involving a complex network of interrelated front companies and legitimate businesses, making it even harder to detect.

Corporate service providers (CSPs) are key gatekeepers against the misuse of companies, and are regulated by ACRA. CSPs provide an additional layer of checks, as they are required to perform CDD when they are engaged to incorporate companies or provide other corporate services. Non-residents must engage a CSP registered with ACRA to incorporate a company in Singapore, which subjects them to the CSP's suite of CDD measures and checks.

Tackling the misuse of companies requires collaboration across the key personnel of companies, gatekeepers like CSPs, ACRA and the relevant authorities.

Enhancements to the regulatory framework for CSPs

In July 2024, the Corporate Service Providers Act 2024 (CSP Act) was introduced to enhance the regulatory framework for CSPs. The key changes included:

- **Requiring all entities carrying on a business in Singapore of providing corporate services to be registered with ACRA as a CSP.** This ensures that all Singapore-based entities that provide corporate services will be regulated by ACRA and subject to AML obligations.
- **Introducing fines of up to \$100,000 for errant CSPs and their senior management** that do not comply with their AML obligations. In certain circumstances, the senior management of CSPs can also be held liable for such breaches and face fines.

These amendments will enable more dissuasive action to be taken against CSPs that are complicit in the misuse of companies for money laundering.

Measures to tackle the misuse of nominee directorship arrangements

The CSP Act also introduced new requirements to tackle the misuse of nominee directorship arrangements:

- **Arrangements to be made by CSPs.** An individual can only act as a nominee director by way of business if the nominee directorship is arranged by a CSP.
- **“Fit and proper” requirements.** The CSP must ensure that the individual it arranges to act as a nominee director is a “fit and proper” person.

These amendments ensure that nominee directorships are held by individuals who can discharge their duties as company directors properly.

ACRA has also continuously enhanced its supervisory and enforcement efforts for individuals assessed to be of a higher risk, such as those holding a large number of nominee directorships and exhibiting other traits of being at-risk. These enhancements have led to the disqualification or debarment of such high-risk individuals.

Strengthen measures to deter misuse of companies

As Singapore's company registry, ACRA oversees the incorporation of about 50,000 companies annually. Checks are conducted to mitigate the risk of incorporating companies likely to be used for purposes that are unlawful or contrary to national security or national interests⁴. However, given the large volume of companies looking to be incorporated annually and the lack of evidence against companies at the point of incorporation, it would not be feasible or practical for ACRA

⁴ This is provided for under section 20(2) of the Companies Act 1967.



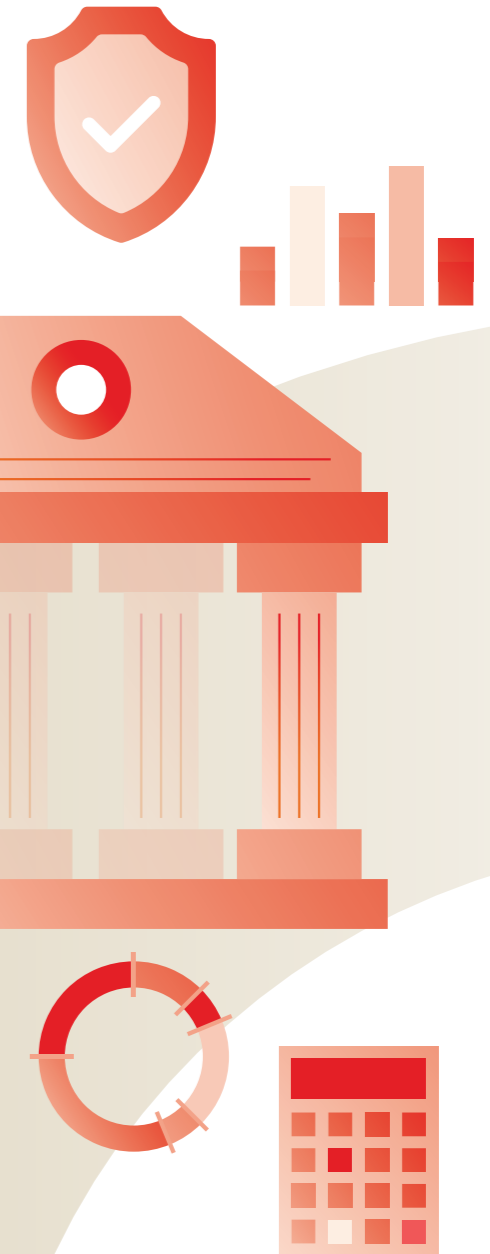
What are nominee directors?

A **nominee director** is a person who is appointed as a company director, but acts according to another person's directions. Nominee directors have the same legal obligations as other directors, such as being required to discharge their duties responsibly, with honesty and reasonable diligence. They will face sanctions if they fail to discharge their duties as directors.

Singapore requires all companies 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 Singapore⁵. Many CSPs provide nominee directorship arrangements to support their overseas-based clients to set up a company in Singapore. This is a legitimate service to fulfil the requirement for an ordinarily resident director.

However, there have been cases where criminals misuse nominee directorship arrangements to create shell companies to facilitate money laundering. To tackle such scenarios, ACRA has introduced requirements for (i) individuals who act as nominee directors by way of business to be arranged by a CSP, and (ii) CSPs to ensure that the individuals they arrange to act as nominee directors are fit and proper. Individuals and CSPs who violate these requirements will have committed an offence.

These new requirements complement the existing sanctions for directors who fail to uphold their legal obligations, such as disqualification and debarment from taking on additional directorships.



⁵ Singapore's requirement for companies to appoint at least one ordinarily resident director goes beyond the requirements of many other jurisdictions.

to impose overly stringent measures without compromising the ease of doing business for the large majority of companies.

ACRA will continue screening prospective companies on a risk-based approach when they apply for incorporation. Where there are clear indicators of illegitimate activities by a prospective company and its individuals, they will continue to be identified, scrutinised and rejected if there is sufficient evidence. For companies where there is some indication but insufficient evidence to conclude they are being set up for illegitimate activities, ACRA, other sector supervisors and gatekeepers will maintain closer supervision over them post-incorporation and take necessary

enforcement actions where appropriate. These complement existing ongoing surveillance, as criminals' nefarious behaviour may only emerge after they have gained a foothold in our economy.

ACRA, in collaboration with other agencies, will also step up their efforts to strike off inactive companies, which could be an indicator of shell companies. After incorporation, ACRA proactively identifies companies that exhibit signs of inactivity, and initiates the process to strike off such companies. ACRA has increased the rate at which inactive companies are struck off (especially for those with higher risk profiles), to mitigate the risk of misuse for money laundering.

KEY OUTCOMES

With these efforts to Proactively Prevent money laundering, gatekeepers will have greater clarity on what is expected of them and be better equipped in preventing money laundering cases.

While these measures will help to reduce the likelihood of money laundering, it is not realistic to expect a complete eradication of all future money laundering cases as there will inevitably be bad actors. We must therefore also enhance our capabilities to detect such cases.

TIMELY DETECTION



Illicit activities usually begin only after bad actors have successfully gained a foothold in our economy. There is often no sign or evidence of nefarious activities at the point of a company's incorporation or its first transaction with a gatekeeper (e.g. when setting up a corporate bank account).

Therefore, a well-functioning AML framework must be supported by strong capabilities to detect and weed out bad actors and illicit activities during or after they take place.

Even as individual gatekeepers and government agencies have deployed more effective AML measures over the years, criminals too have learnt to exploit information gaps to conceal the illicit nature of their transactions and activities.

The responsible sharing of relevant information amongst gatekeepers and agencies is thus increasingly important in combatting money laundering. We have reviewed how to enhance information sharing to strengthen sensemaking among government agencies, and between government agencies and gatekeepers.

Sensemaking in the public sector

As Singapore's Financial Intelligence Unit (FIU), the STRO analyses and enriches information from priority STRs, and produces financial intelligence reports that are disseminated to relevant law enforcement



agencies and sector supervisors. These reports provide actionable intelligence for relevant authorities to take the appropriate enforcement or regulatory actions.

Sector supervisors also receive significant volumes of information daily which may be useful for AML purposes. Sector supervisors apply advanced data analytics techniques and technologies to pick out risk signals from the voluminous data they receive.

In complex cases where criminal activities span multiple sectors and are overseen by different government agencies, data from a single agency may reveal unusual transactions or behaviour patterns, but may not conclusively indicate illicit activities. Agencies will need to triangulate this data with information from multiple sources, including other agencies, to more effectively identify discrepancies that may indicate an intent to conceal criminal activities.

Sensemaking among gatekeepers

Gatekeepers such as financial institutions, real estate salespersons and estate agencies, PSMDs, lawyers and corporate service providers are key in detecting suspicious activities. They have unique insights into their customers' behaviour because they interact directly with them.

Strong partnerships between the public and private sectors strengthen our collective ability to detect suspicious activities and emerging risks promptly. For instance, STRO regularly engages gatekeepers to share emerging financial crime typologies and guide gatekeepers on how to file better STRs.

There are also other public-private partnerships:

- **The AML/CFT Industry Partnership (ACIP) brings together the financial sector, regulators, law enforcement agencies and other government agencies to collaboratively identify, assess and mitigate key and emerging money laundering risks facing Singapore.** Co-chaired by MAS and the Commercial Affairs Department (CAD) of the Singapore Police Force, ACIP has enhanced the AML/CFT measures for Singapore's financial sector through

its initiatives, such as the publication of best practices papers for financial institutions in key risk areas.

- **In April 2024, with the trust and experience built up through the sharing in ACIP, MAS launched the Collaborative Sharing of Money Laundering/Terrorism Financing Information and Cases (COSMIC) platform, which augments ACIP's efforts.** COSMIC is a digital platform that MAS co-developed with six major banks in Singapore. It allows participating financial institutions to share with one another, information on customers who exhibit potential financial crime concerns. MAS is closely engaging participant financial institutions to identify and address any operational concerns during its initial phase, which will last for two years.
- We have reviewed existing and planned enhancements to information-sharing mechanisms. **We recommend additional measures to improve the ability of sector supervisors and gatekeepers to engage in the Timely Detection of illicit activities.**



Key Facts

COLLABORATION BETWEEN AGENCIES AND PRIVATE SECTOR TO TACKLE A NETWORK OF LEGAL PERSONS USED TO LAUNDER SCAM PROCEEDS

In the second half of 2020, the CAD observed a rise in Business Email Compromise (BEC) scams targeting foreign companies, with Singapore corporate bank accounts used to receive the fraudulent proceeds. Through a deep dive network analysis, CAD uncovered a large network of shell companies incorporated in Singapore, which did not have any legitimate business transactions and were suspected to be receptacles to be deployed for laundering illicit funds. These shell companies were observed to be created by a few CSPs.

CAD established that most of the victims were corporates based overseas. The allegedly fraudulent funds were received in the Singapore bank accounts of these shell companies, and a large proportion of these funds were transferred to other corporate bank accounts in another country (Country X) within one or two days. By February 2021, CAD had received more than 80 reports, involving approximately \$141 million, that could be linked to this network.

CAD flagged this case for whole-of-government (WOG) mitigation action, which triggered a joint project between CAD, MAS and relevant members of ACIP. Specific intelligence and leads were shared with the banks for them to surface new leads and to conduct further analytics. **This information sharing led to over 990 STRs filed by ACIP members, which STRO analysed and disseminated to CAD to augment investigations.**

These efforts, coupled with CAD's close relationship with the foreign authorities and the ability of the Singapore law enforcement agencies to initiate immediate freezing actions, enabled Singapore authorities and banks to intercept about \$71 million worth of fraudulent funds. This included over \$27 million of incoming funds that were blocked by banks' proactive identification of suspicious accounts.

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

ACRA had also investigated and/or inspected the CSPs involved. ACRA had cancelled the registration of two Registered Filing Agents (RFAs) and two Registered Qualified Individuals (RQIs) and imposed financial penalties on six RFAs, ranging from \$4,000 to \$14,000 for AML-related breaches. ACRA also shared information with CAD on an additional 25 individuals who were linked to the case, which had not surfaced in CAD's investigations.

To raise AML awareness among the industry, CAD, MAS and ACIP issued an ACIP advisory on the emerging typologies involving professional ML and misuse of legal persons.

REVIEW & RECOMMENDATIONS



1 Strengthen sensemaking and information-sharing mechanisms within government

Information sharing amongst government agencies is well-established and has delivered success. Nonetheless, there is room to refine these mechanisms to help our agencies more swiftly identify risks and concerns, by ensuring that they exchange and analyse the relevant data promptly.

We will continue improving how we share information between government agencies.

Granting supervisors access to STRs filed by supervised gatekeepers

In August 2024, legislative amendments were made to the CDSA to allow all sector supervisors to access any STRs filed by their regulated entities⁶. This will provide deeper insights on key sectoral risks and trends to supervisors, such as ACRA and CEA. These insights will complement the existing data available to the supervisors, and allow for more effective upstream supervisory and regulatory actions.

Granting STRO access to tax and trade data

Tax and trade data may reveal information on criminal activities, such as tax fraud or money laundering through false trade transactions.

Through the legislative amendments to the CDSA, IRAS and Customs will be able to share tax and trade data with STRO. These data will augment STRO's analyses of money

laundering risks and provide richer intelligence to relevant law enforcement agencies and sector supervisors.

Building bilateral data-sharing channels across government agencies

Agencies are implementing structured bilateral data exchange targeted at specific risks and typologies, to speed up detection of money laundering risks. This enables agencies that have complementary roles in preventing money laundering to share early risk indicators and take swift actions on such entities.

For example, ACRA and MOM have enhanced their bilateral data exchange, to mitigate the risks related to bad actors legitimising their identity in Singapore by using corporate structures and work passes. The data focuses on higher risk entities which may be in breach of existing regulations, including their attributes and their compliance history. Using data analytics, both agencies will identify the potential misuse of companies for fraudulent work pass applications and other regulatory violations, for supervisory and enforcement follow-ups.

Insights from these bilateral information exchanges may then be shared with the broader group of agencies to facilitate WOG sensemaking.

Development of a WOG interface for the data sharing on money laundering

Criminals may adopt sophisticated means to avoid detection. They may layer their activities

across different sectors and use different front entities. While traces of suspicion may be left in their interactions with individual agencies, these traces alone may not be sufficient to raise concerns. A more revealing picture may emerge when these traces are triangulated and pieced together with information from multiple sources, to more effectively identify anomalies or discrepancies.

To facilitate more timely and comprehensive sensemaking of money laundering risks across government agencies, we will develop a new WOG data sharing interface, NAVIGATE (National AML Verification Interface for Government Agencies Threat Evaluation), led by SPF.

Using NAVIGATE, law enforcement agencies, sector supervisors and other relevant agencies can seamlessly screen against one another's databases and expeditiously assess entities of concern for ML risks. This replaces the current ad-hoc data requests between agencies, which can be cumbersome and have a limited scope. NAVIGATE enables agencies to promptly identify and deal with individuals and entities of concern, and collectively develop a timelier and more comprehensive picture of potential ML risks.

To safeguard data confidentiality and ensure appropriate use of information, there will be strict terms and rules on access to and use of NAVIGATE. We will roll out NAVIGATE progressively to meet near-term needs, while keeping pace with new challenges that might emerge over time.

Establishment of an inter-agency workgroup to aid sensemaking of money laundering

We will also establish an AML Sensemaking Workgroup, to keep the Government's operational policies, data sharing processes and capabilities in sensemaking up-to-

date and robust against emerging and sophisticated ML typologies. The Workgroup, led by MHA and SPF, will complement data-sharing on NAVIGATE and strengthen inter-agency case coordination (which we will elaborate on as a measure under Effective Enforcement).

To complement the shift towards a data-focused approach to detect money laundering risks, SPF will lead training across agencies, to strengthen agencies' sensemaking capabilities, including using technology and data analytics.

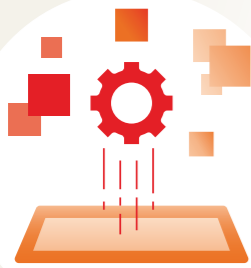
2 Deepen channels for data sharing amongst and with gatekeepers

We will continue to explore ways to expand data sharing among and with private sector gatekeepers, given their key role in combatting money laundering through their dealings with clients.

Such initiatives should be carefully calibrated. Some general principles are:

- The **nature** of the data shared must be relevant to gatekeepers and appropriate for sharing. Data privacy and sensitivity concerns must also be appropriately mitigated.
- The recipients of the data must be kept to a **restricted audience**. Data should only be shared with gatekeepers who have a legitimate use case, such as for risk assessment of their clients.
- The appropriate **guardrails** must be in place, to prevent unauthorised sharing and disclosure.

⁶ This was previously only allowed for MAS, MinLaw and the Gambling Regulatory Authority, as provided for in their respective regulations.



COSMIC:
Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases

Digital platform where financial institutions (FIs) share information to detect and deter criminal activities

FOCUS ON 3 PRIORITY RISKS FACING SINGAPORE



Misuse of Legal Persons



Trade-based Money Laundering



Proliferation Financing

ROBUST LEGAL FRAMEWORK WITH SAFEGUARDS

Purpose of Sharing



Only for detection and deterrence of ML/TF/PF*



To assess potential financial crime concerns



FIs detect "red flag" indicators of serious financial crime



Provided stipulated thresholds are met

*ML - Money Laundering, TF - Terrorism Financing, PF - Proliferation Financing

HOW DOES COSMIC WORK?

FI detects red flag indicators that cross the stipulated threshold



requests information from other FIs with links to the customer or transaction to assess unusual activities

FI detects multiple red flag indicators that cross a higher stipulated threshold



provides information to other FIs with links to the customer or transaction

FI files a suspicious transaction report to authorities and decides to exit an account



places an Alert on this customer on a "watchlist"

HOW MAY INFORMATION FROM COSMIC BE USED?

By Participant FIs

To identify bad actors and take prompt action to disrupt criminal activities and network

To complement their risk assessment of a customer

By MAS and STRO¹

To support supervision and risk surveillance of the financial system

To support law enforcement efforts

¹The Suspicious Transaction Reporting Office (STRO) is Singapore's Financial Intelligence Unit under the Singapore Police Force that analyses and disseminates financial intelligence to law enforcement and regulatory agencies.

MAS will consider expanding COSMIC platform after initial phase

MAS plans to expand COSMIC in phases, with the initial phase to last for two years. MAS will subsequently evaluate whether to expand COSMIC's coverage to more focus areas and financial institutions.

Non-compliant companies to be flagged

ACRA is intensifying its efforts to strike off inactive companies (especially those with higher risk profiles) to mitigate the misuse of companies. That said, it is not feasible to strike off all companies that exhibit signs of inactivity, as such indicators may not always be conclusive. For instance, an active company could have genuinely missed filing its annual return due to human error.

As an intermediate step, **companies that exhibit signs of inactivity (such as non-filing of annual returns) will be flagged on ACRA's registry.** This will alert gatekeepers to potential risks, support them in their risk profiling and facilitate their calibration of CDD efforts accordingly.

Companies will generally not be struck off unless they are repeatedly non-compliant, as one-off non-compliance may be inadvertent. If companies rectify their non-compliance or close their business, they will no longer be flagged.

Enhancements to ACRA's beneficial ownership framework

ACRA currently requires companies and Limited Liability Partnerships (LLPs) to file information on their **registrable controllers** in the Register of Registrable Controllers (RORC). This information is accessible to government agencies for law enforcement purposes in Singapore and ensures that persons exercising control of companies behind the scenes are known to authorities. This is useful for risk-profiling companies, especially during investigations.



Who is a Registrable Controller?

The Registrable Controller (also commonly referred to as a **beneficial owner**) of a company or an LLP is an individual who:

- has an interest in more than 25% of shares in a company; or
- holds more than 25% of members' voting rights in a company; or
- can exercise significant influence or control over a company/LLP.

ACRA is further enhancing Singapore's beneficial ownership framework. In July 2024, the Companies and Limited Liability Partnerships (Miscellaneous Amendments) Act 2024 was passed to improve the accuracy of information in the RORC:

- All new companies are required to maintain information on their beneficial owners from the date of their incorporation, instead of the previous requirement to only do so within the first 30 days of incorporation.
- Companies are required to verify and update their beneficial owners' information annually.

- The maximum fine for offences related to registers was increased from \$5,000 to \$25,000, to deter companies from failing to maintain their registers, keep the information up-to-date or correct inaccurate information.

ACRA will continue to build on its efforts and develop the next phase of Singapore's beneficial ownership framework. This includes working with industry partners to study if the beneficial ownership information could be a useful additional source of information to support key gatekeepers such as banks in tackling money laundering, while considering the sensitive nature of the data.

KEY OUTCOMES

Through Timely Detection, supervisors will gain access to stronger sensemaking capabilities, which will potentially allow our agencies to detect money laundering cases earlier. We will also continue to explore how we can share data with the relevant gatekeepers.

Upon detecting illicit activity, law enforcement and supervisors must have the resolve to take decisive enforcement action against the criminals and negligent gatekeepers respectively.

EFFECTIVE ENFORCEMENT



The Government's robust stance against money laundering is underscored by our commitment to take decisive enforcement actions. Our law enforcement agencies (LEAs) are empowered under our laws, including the CDSA and Criminal Procedure Code 2010 (CPC), to pursue and prosecute money laundering offences. There is also a wide range of tools available to sector supervisors, to act against AML breaches within their respective sectors. The punishments and penalties include imprisonment, forfeiture of assets, fines, regulatory penalties, and cancellation of licences or permits.

Money laundering is often transnational in nature, particularly in a global trade and financial centre like Singapore. Most of the monies laundered in Singapore originate from overseas criminal activities, such as online scams and illegal gambling operations. Singapore's LEAs work closely with foreign counterparts to gather evidence on the criminal conduct of the suspects, to trace and interdict illicit proceeds in Singapore.

Nevertheless, money laundering typologies are constantly evolving. Criminals are finding new ways to evade detection. They often move monies across multiple jurisdictions to evade and frustrate efforts by LEAs globally, taking advantage of technological innovations. To ensure our enforcement levers remain relevant and effective, we must nimbly and regularly update our levers and toolkits.

Learning from recent money laundering cases domestically and internationally, and referencing latest international standards set by the FATF, we have refreshed our legislative levers and toolkits to provide the Government with the ability to better calibrate enforcement action against money laundering offences.

We have also identified our key emerging risk areas, and are implementing measures to enhance the deterrence of our laws and frameworks, and ensure that our system remains effective.

We reviewed existing and in-progress measures to take Effective Enforcement action against criminals, and identified recommendations to tackle illicit activities.

REVIEW & RECOMMENDATIONS



1 Enhance legislative levers for law enforcement agencies to better pursue and prosecute ML offences

LEAs face some challenges when prosecuting money laundering offences. For example, there is a high threshold to successfully prove that a suspect's proceeds arise from foreign criminal conduct, given the need for evidence from foreign authorities or entities.

With the passage of the Anti-Money Laundering and Other Matters Act (AMLOM Act) in August 2024, which included amendments to various legislation such as the CDSA and CPC, LEAs will have more effective levers to prosecute money laundering cases arising from foreign criminal conduct and deal with the seized properties of absconded suspects.

Enhanced levers to prosecute money laundering cases arising from foreign criminal conduct

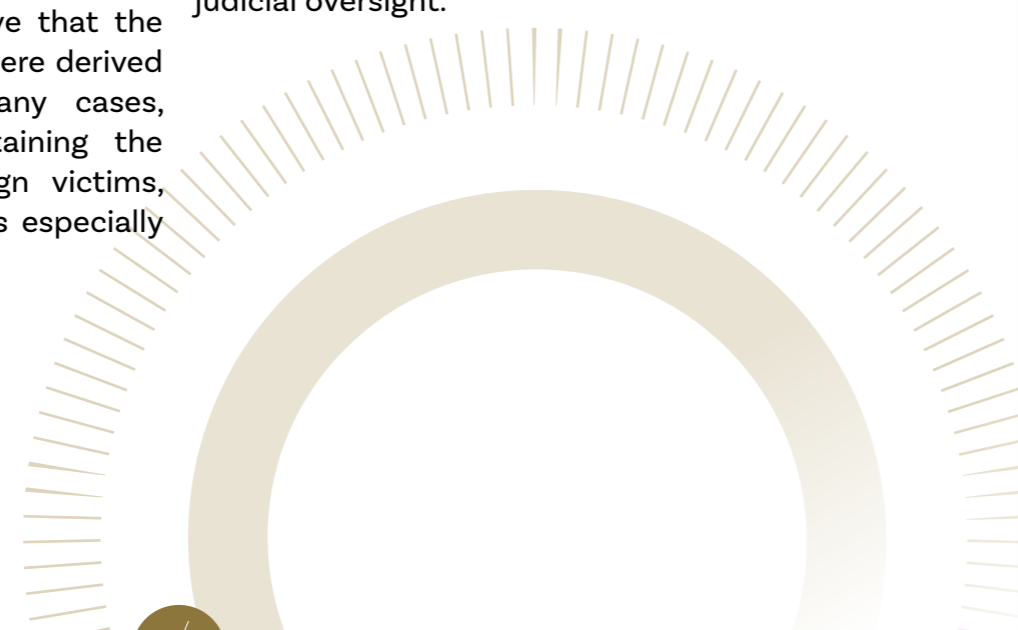
Previously, LEAs needed to prove that the monies laundered in Singapore were derived from criminal conduct. In many cases, LEAs faced challenges in obtaining the necessary evidence from foreign victims, entities and authorities. This was especially

so if the criminal proceeds had flowed through multiple bank accounts or foreign intermediaries before entering Singapore, which is often the case.

With the amendments to the CDSA in August 2024, it will suffice for the Prosecution to prove that the money launderer knew, or had reasonable grounds to believe that the property he was dealing with were the gains from criminal conduct.

Enhanced levers to deal with seized properties of absconded suspects

Targeted amendments to the CPC were made to enable the Government to better deal with absconded suspects. Under the AMLOM Act, an absconded person reasonably suspected of having committed a relevant offence in connection with property seized by the authorities cannot claim to be entitled to the property, unless the person personally presents himself or herself before a law enforcement officer to assist in the investigations. The process is subject to judicial oversight.



Key Facts

HOW ENHANCED LEVERS TO THE CDSA WOULD ENABLE LEAS TO BETTER PROSECUTE ML CASES ARISING FROM BUSINESS EMAIL COMPROMISE (BEC) SCAMS*

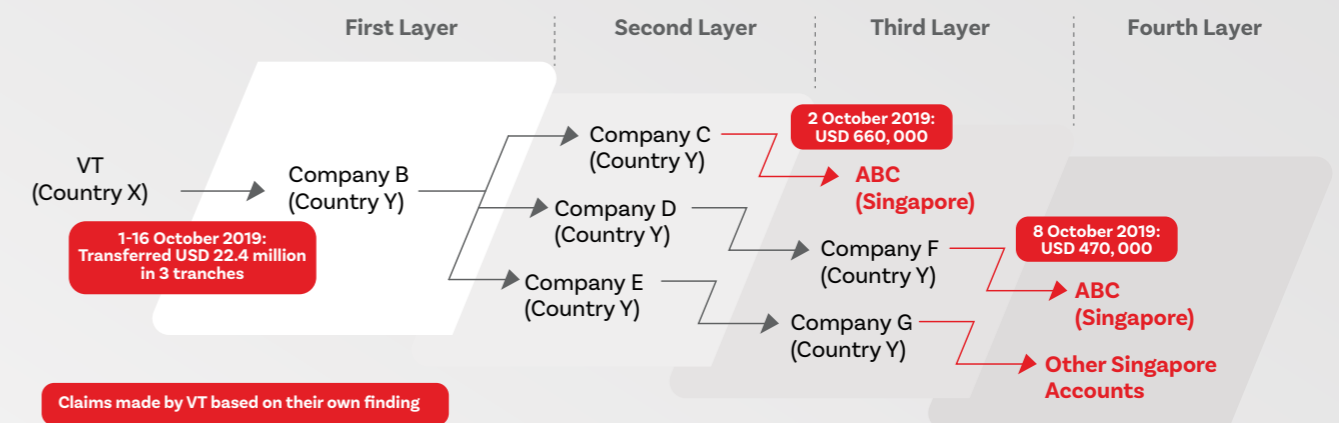
BEC scams are a global phenomenon, which the FBI announced had caused business losses of \$50 billion between 2021 and 2022. The amendments would enable the authorities to pursue prosecution more effectively and steadily against BEC scammers.

For example, Police received a letter from **VT**, a listed company incorporated in Country X in April 2020. **VT** claimed that they were the victim of a BEC scam and they had sent a total of \$30.2 million to a bank account in Country Y. **VT** claimed that the monies they sent to Country Y were eventually sent to Singapore. The monies were sent to Country Y in October 2019. Between October 2019 and April 2020, **VT** carried its own investigations, obtaining information through disclosure orders from the courts in Country Y. Police commenced investigations into the Singapore bank account that belonged to **ABC Pte Ltd**.

In the course of Police investigations, the local director of **ABC** admitted that he had given up the control of his bank account to an unknown person, and had allowed **ABC's** bank account to be used to receive and transfer funds, which he suspected to have come from illegal sources. However, key banking information was not available or forthcoming from the foreign banks to allow Police to form a funds trail directly attributing the money in **ABC** to **VT**. Additionally, given the time lapse, monies had already been dissipated from **ABC's** account. With no prospect of recovery, **VT** had no incentive to continue to cooperate with Police.

Prior to the AMLOM Act amendments, the above alone was insufficient to prosecute the director of ABC for ML offences. AGC also had to show that the monies in ABC's account were: (i) derived from criminal conduct against VT; and (ii) that the monies could be directly linked to VT.

The amendments to the CDSA will allow for prosecution against **ABC**, given that the local director of **ABC** had admitted to the ML offence and there is evidence that the monies could have been derived from the BEC scam against **VT**.



*In BEC scams, scammers impersonate the victims' colleagues, boss, business partners or suppliers via a hacked email account or spoofed email address. Victims will be instructed to make payments to a bank account which the scammer will provide, on the pretext that there is some problem with the usual banking facility.

Previously, such suspects could have frustrated investigative efforts, by not returning to Singapore and hoping that the Court would eventually order the release or disposal of the seized property. Publication of the National Asset Recovery Strategy.

Publication of the National Asset Recovery Strategy

The Government has made asset recovery a key priority in our national AML framework, to maximise the forfeiture of assets and provide restitution to the victims.

In June 2024, Singapore published the **National Asset Recovery Strategy (NARS)**, which provides clearer guidance and operational focus to all LEAs in pursuing asset recovery.

The NARS focuses on four operational pillars to:

- **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.

The strategy enhances LEAs' operational capabilities in pursuing asset recovery, which in turn removes the financial incentives for criminals to launder their illicit proceeds through the Singapore financial ecosystem.

2 Continuously review penalty frameworks to ensure they remain proportionate and dissuasive

As part of the Government's ongoing reviews of Singapore's AML laws, we have enhanced our penalty frameworks, to more effectively take criminals to task and deter would-be criminals.

Enhancements to sanctions for breaches of obligations by gatekeepers

As part of the CSP Act that was introduced in July 2024, CSPs and their senior management who breach their AML obligations will face stricter sanctions:

- CSPs that are non-compliant with their obligations to detect and prevent money laundering will now face a fine of up to \$100,000 – a four-fold increase from the previous financial penalty of \$25,000.
- The senior management of CSPs can also be held liable for such breaches under certain circumstances⁷, and face a fine of up to \$100,000.

Other supervisory agencies, such as CEA, URA and MinLaw, will also clarify or enhance the AML penalty frameworks for their respective gatekeepers⁸, to ensure that the penalties meted out are commensurate with the severity of breaches and culpability of the offenders.

⁷ For example, if they knew or ought reasonably to have known that the offence would be or is being committed but failed to take all reasonable steps to prevent or stop the commission of that offence.

⁸ Real estate salespersons and agencies, property developers and lawyers.

Enhancements to the reporting of cross border movements of physical cash

Moving large amounts of physical cash across borders is one method of money laundering, as it bypasses financial institutions and obscures the origins of the funds.

Under the Cross Border Cash Reporting Regime (CBCRR), individuals are required to declare cross border movements of physical cash and bearer negotiable instruments (CBNI) that are above the FATF-prescribed threshold of \$20,000.

In May 2024, we enhanced the CBCRR, by:

- **Increasing the composition fines imposed for CBCRR offences by threefold**, which aligns our measures with international comparisons; and
- **Mandating the electronic submission of CBCRR declarations for travellers entering and leaving Singapore**, which will facilitate more timely detection of suspicious activities.

These efforts will increase the dissuasiveness of the CBCRR's punitive sanctions and better stamp out money laundering activities that leverage cross border movement of physical CBNI.



Key Facts

ENFORCEMENT ACTIONS AGAINST BREACHES OF THE CROSS BORDER CASH REPORTING REGIME

SPF and Immigration and Checkpoints Authority (ICA) regularly mount joint enforcement operations to better detect and deter CBCRR breaches at our checkpoints.

During the most recent CBCRR joint operations at the airport from 17 to 23 June 2024, 10 travellers were caught moving cash exceeding \$20,000 (or its equivalent in foreign currencies) into Singapore without declaration, two travellers were issued with Notices of Warning, while six travellers were issued with composition sums amounting to \$23,000 in all.

Investigations were launched against two travellers who carried money of various physical currencies, exceeding \$140,000 in total, into Singapore without declaration.

3 Strengthen inter-agency coordination to enable swifter and more effective action against illicit ML activities

The Government coordinates actions on priority ML cases through the Inter-Agency STR Analytics (ISTRA) taskforce, which comprises selected supervisory and law enforcement agencies. Members surface significant cases with a nexus to other agencies, and collaborate to take supervisory and enforcement action

against major criminal networks. ISTRA is part of the broader Risk & Typologies Interagency Group (RTIG), which reports to the AML/CFT SC.

Expansion of inter-agency coordination across agencies to effectively enforce against money laundering

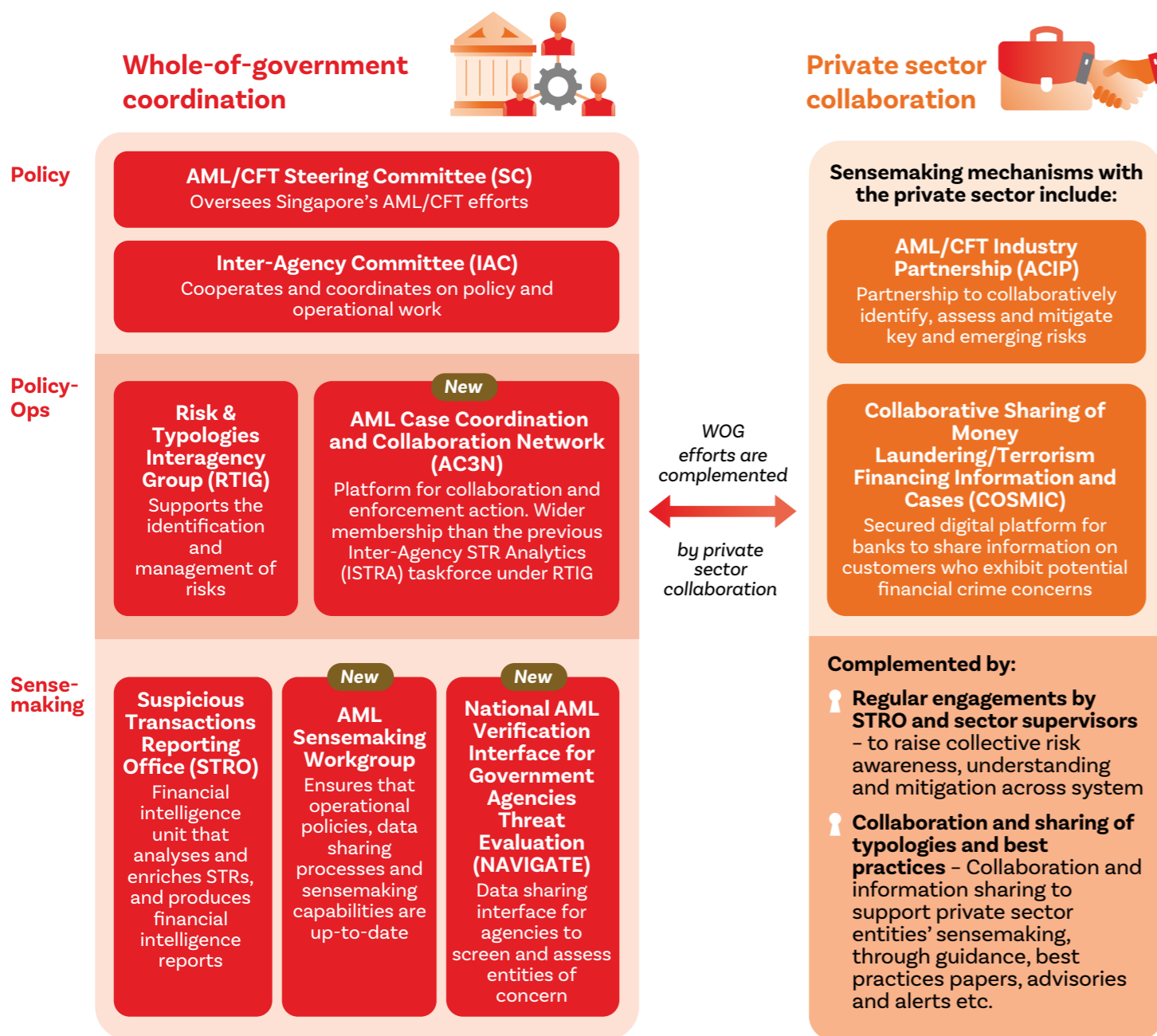
To enable more effective and coordinated supervisory and enforcement actions to be taken by agencies at the WOG level, **the Government has evolved ISTRA by bringing all government agencies involved**

in combatting money laundering into a new AML Case Coordination and Collaboration Network (AC3N).

With a wider membership and a higher level of oversight than ISTRA, AC3N will be able to more quickly “connect the dots” on cases with a nexus to multiple industry sectors and government touchpoints, and pursue a

wider range of measures against criminals and bad gatekeepers.

Through their AC3N participation, sector supervisors will also gain deeper insights into risks affecting their specific sectors. These insights will drive supervisory efforts, and be shared with gatekeepers to bolster Singapore’s collective AML defences.



KEY OUTCOMES

Our measures seek to enable Effective Enforcement against money laundering cases. LEAs and sector supervisors will have closer coordination and a greater awareness of cross-sectoral risks. LEAs will also have stronger levers to pursue and prosecute money laundering offences, and sector supervisors will enhance their penalty frameworks.

The IMC’s recommendations and measures will fortify our defences in a holistic and complementary manner. They will ensure that we can take appropriate measures when – not if – criminals attempt to launder their illicit assets in Singapore.

CONCLUSION

Money laundering is a persistent and evolving challenge to all international financial centres, as criminals seek destinations that are open and well-connected to hide their illicit assets.

Singapore is committed to uphold our hard-earned reputation as a trusted financial system and business hub, through our robust and effective approach to combatting money laundering and other financial crimes. We have put our commitment into action by proactively strengthening our AML framework over the years.

The IMC's recommendations are the latest salvo in our battle against financial crime, but they are neither exhaustive nor final. We are under no illusion that we can completely prevent money laundering, as criminals will adapt their tactics. But we will be alert to these tactics, keep our AML framework up to date and bring these criminals to justice when we detect them.

As a society, we must all remain watchful and vigilant. All stakeholders, from government agencies to gatekeepers, and businesses to individuals, are key in the fight against money laundering. With our collective partnership, we will continue to act decisively to combat money laundering, while remaining welcoming to legitimate investors and businesses.



