MINISTRY OF LAW
SINGAPORE

MinLaw Industry Compliance Engagement (MICE) 2026

21 May 2026

- **Music is playing in the background now. Please check your audio settings and volume for your speakers/ headphones if you are not able to hear it, or exit and rejoin the session.**
- **Attendees are not required to switch on their videos. Your mic is muted for the session.**
- **If you face any Zoom technical difficulties, please ask in the Q&A Zoom feature.**

Programme

If you have any questions relating to today's session, please leave your queries via the Q&A function.

We will try to reply to your question or address them during the Q&A segment at the end of the session.

Audience poll
Segment 1:
• Insights/Findings from Singapore's FATF Mutual Evaluation

• Further Guidance
  • Proliferation and Terrorism Financing Risk Awareness
  • Trustees' AML/CFT/CPF Obligations

Programme

If you have any questions relating to today's session, please leave your queries via the Q&A function.

We will try to reply to your question or address them during the Q&A segment at the end of the session.

Segment 2:

- Further Guidance
  - CDD and ECDD Obligations
  - Cash Equivalent
  - Suspicious Transaction Report (STR)
- PSMD Enforcement Statistics
- Case studies
  - Conducting Regulated Dealing Without Registration
  - Acceptance of Virtual Currency Payment
  - Failure to Conduct ECDD
  - Cancellation of PSMD Registration

Programme

If you have any questions relating to today's session, please leave your queries via the Q&A function.

We will try to reply to your question or address them during the Q&A segment at the end of the session.

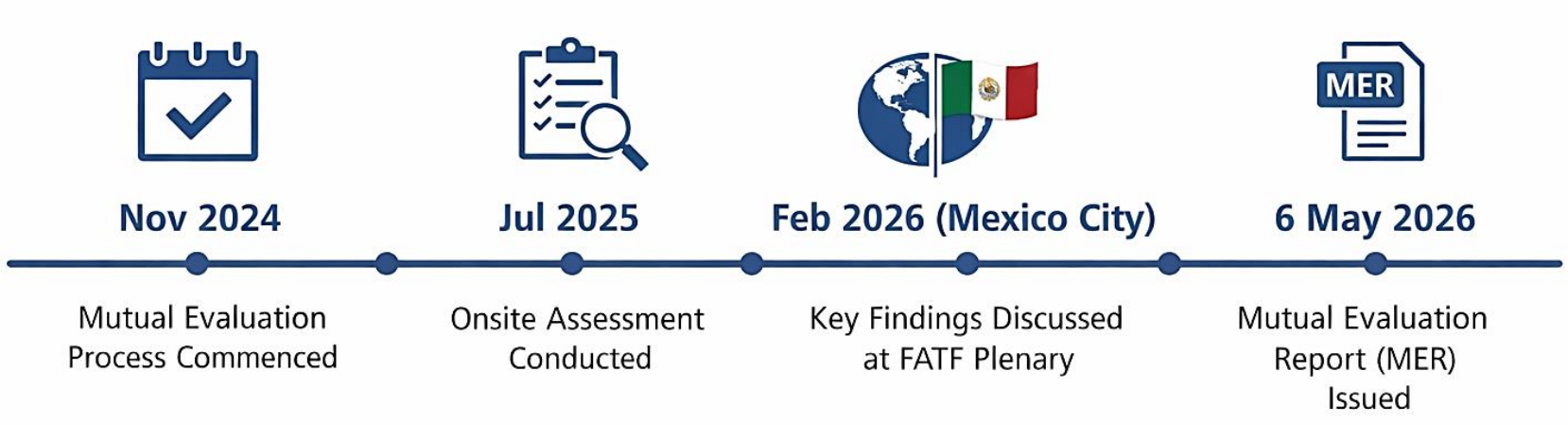
Segment 3:
• CSA Sharing: Introduction to Cybersecurity Health Clinic
• SPF Anti-Scam Centre Sharing: Anti-Scam Briefing
• Code of Practice on AML measures to combat scams
Kahoot! Quiz
Q&A
Poll

Singapore's 5th Round FATF Mutual Evaluation

Ministry of Law

Singapore's 5th Round FATF ME

Assessment of Singapore's AML/CFT/CPF Regime against FATF Standards



Behind the scenes….

- Preparation for the Mutual Evaluation began in **2020**, involving **over 26 government agencies**, and industry associations.
- **Regulated entities across 24 sectors**, including PSMDs, pawnbrokers and moneylenders, have strengthened their **ML/TF/PF risk awareness** and understanding of **AML/CFT/CPF obligations**.
- This collective effort underpins Singapore's AML/CFT/CPF framework and outcomes.

Positive ME Outcome - Singapore's AML/CFT/CPF Framework assessed to be in line with FATF's Expectations

Possible Outcomes from Assessment

FATF ME Assessment

Regular Follow-Up
Default monitoring mechanism

5th Round ME

Enhanced Follow-Up
For countries that needs major improvement or more intensive follow-up

4th Round ME (in 2016)

International Cooperation Review Group (ICRG) Process
For countries that need fundamental improvements/with strategic deficiencies in their AML/CFT/CPF regime

Refer to the published MER at the FATF Website for more details

Key Takeaways from Singapore's 2026 ME Report

Strengths of Singapore's AML/CFT Regime

- ✓ **Robust AML/CFT legal framework** with **sound risk understanding**
- ✓ **Strong public-private collaboration** on AML/CFT efforts, leading to improved risk understanding and compliance culture
- ✓ DNFBP sector supervisors generally demonstrate **reasonably sound risk understanding**
- ✓ DNFBP sector supervisors are active in promoting DNFBPs' understanding of ML/TF risks and AML/CFT obligations through **guidance and outreach**. ("A strength of Singapore's regime.") MinLaw's **screening module in *my*Pal** recognized as assisting smaller PSMDs with their targeted financial sanction (TFS) obligations
- ✓ **Improvements in the overall compliance culture** of the private sector observed, with some positive outcomes as DNFBP sectors demonstrate **improvements in risk understanding** and **gradual improvements in AML/CFT controls** for newly regulated sectors.

Key Takeaways from Singapore's 2026 ME Report

Areas for Improvement

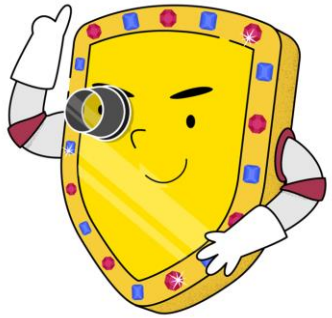
- **Relatively higher** levels of breaches by **PSMDs** relating to **risk assessment (RA)** and other **AML/CFT requirements** (e.g., **CDD/ECDD, record-keeping, IPPC**).

- Relatively **low numbers of STRs** submitted by moneylenders, PSMDs and pawnbrokers. A large proportion (45%) of STRs filed by PSMDs and pawnbrokers arose from **adverse news** (rather than ML/TF/PF red flag indicators). Deficiencies related to **PSMDs not maintaining an active SONAR account**.

- DNFBPs displayed **uneven understanding** of **TF and PF TFS** obligations; some unsure what to do when there was a positive match. Less consideration given to **complex PF sanctions evasion techniques**.

- **Penalties imposed** for **unregistered regulated dealing** and **AML/CFT/CPF offences** could be **more dissuasive**.

Going Forward…



How We Can Do Better

- Continue to **keep abreast of AML/CFT/CPF developments** and implement adequate mitigating measures.
- **Stay vigilant** and recognize **ML/TF/PF red-flag indicators**, and **complex PF sanctions-evasion typologies**.
- Maintain an **active SONAR account** and **file STRs** where ML/TF/PF or illicit funds are suspected.
- Develop, implement and update your **RA** and **IPPC.**
- Conduct **CDD/ECDD**, **submit CTRs promptly and comply with record-keeping** requirements.
- **Subscribe to MAS website** to be alerted to changes to sanction/ alert lists immediately
- **Screen** customers and related parties against sanction/ alert lists.
- **Do not transact** with **designated** persons/ entities; **freeze funds or assets immediately**, and **file an STR**.

Private Sector Support for the ME Assessment

Thank you!

Fund Express (Tekka) Pawnshop Pte. Ltd.

Maxi-Cash

MONEYMAX

Thai Hong Pawnshop Pte Ltd

TOP CASH

BTB CREDITZ LICENSED MONEYLENDER

CF Money Pte Ltd

Lending Bee®

Online Credit Pte Ltd licensed moneylender

PR VR Capital Pte Ltd

Quick Credit Pte Ltd®

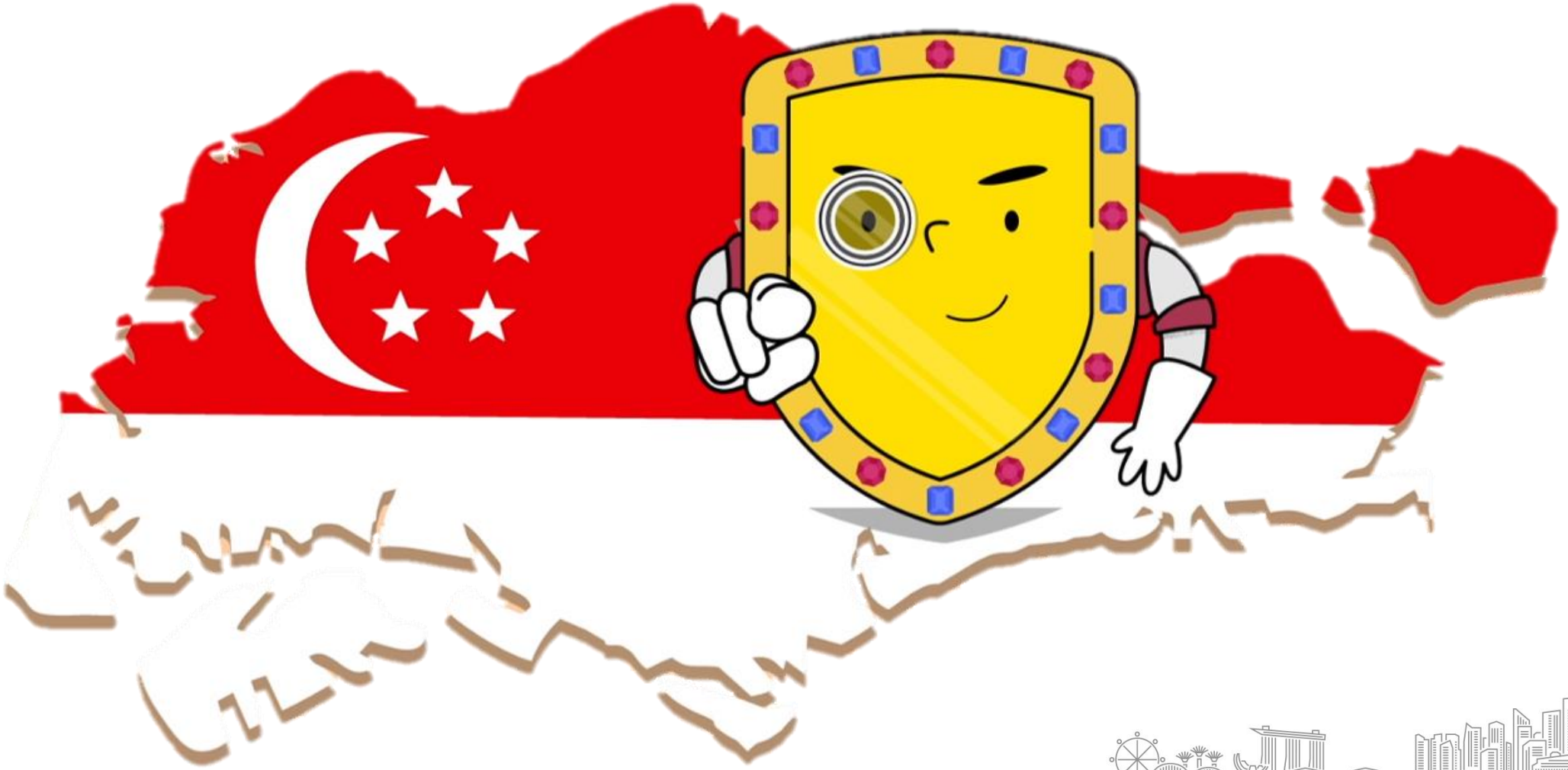
THE HOUR GLASS

METALOR®

MONEYMAX JEWELLERY

Names in alphabetical order

Strengthening Singapore's AML/CFT/CPF System Together



Proliferation Financing

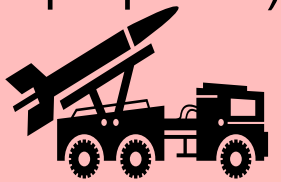
Definition of Proliferation Financing (PF)

PF refers to the act of **raising, moving or making available funds, assets or economic resources to support the development or acquisition** of weapons of mass destruction (WMD)

PF risks arise from activities such as:

Manufacturing, transporting, exporting and stockpiling of nuclear, chemical and biological weapons

Means of delivery and related materials (including technologies and dual-use goods for non-legitimate purposes)



What are your PF obligations?

Do not enter into transactions with designated individuals or entities under targeted financial sanctions

Ascertain if your customer or any related person is a sanctioned individual or entity

Freeze any assets immediately

File an STR immediately, or within 1 business day

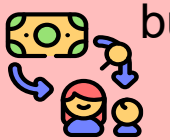
Watch out for sanctions evasion red-flags

Ensure you are **subscribed to the MAS website** to receive updates on the relevant sanctions lists

Red Flag Indicators: Sanctions Evasion Activity

Use of cash or precious metals (e.g. gold) to purchase industrial items

Commercial business behaving like a money-remittance business



Small trading, brokering or intermediary company acting inconsistently with its normal business

Customers or counterparties are linked or coordinated

Evidence of fake or fraudulent documents

Use of personal accounts to purchase business or industrial related items

SCAN HERE

For more red flags indicators, refer to Annex D of the Guidelines for Regulated Dealers

Example of a Complex PF Evasion Technique

Terrorism Financing

What is Terrorism Financing (TF)?

Act of providing funds to terrorists to carry out acts of terrorism

- Sources of funds for TF may be legitimate or illegitimate.
- Scan to find out more about TF risks in Singapore's context.

SCAN

GO.gov.sg

Singapore's key TF threats include:

Terrorist groups such as ISIS, Al-Qaeda, Jemaah Islamiyah

Potential spillovers from geopolitical tensions, especially in the Middle East

Radicalised individuals, including self- radicalised persons sympathetic to terrorist causes

Methods of Exploitation for TF

Precious stones and precious metals

- To move high-value items across borders
- Items are high in value and may be small in size

Digital payment tokens / virtual assets

- To raise and move funds quickly across borders

Cash couriers

- To physically move funds across borders

Terrorist financiers may use one or more methods to obscure or complicate the tracing of the source of funds for TF

Trustees' AML/CFT/CPF Obligations

Trustees' AML/CFT/CPF Obligations

Residual Trustees

- Refers to non-professional trustees (i.e. not licensed trust companies, banks, or other regulated financial institutions)
- Subjected to AML/CFT/CPF obligations under Part 7 of the Trustees Act and the Trustees (Transparency and Effective Control) Regulations

Obligation

- Residual Trustees **must inform the specified person** (e.g. regulated dealer) that they are acting for a **trust before forming a relationship or before entering into a transaction exceeding $20,000**

Remember to...

To share information with Residual Trustees on their obligations

Share this link with Residual Trustees, which you may come into contact with, where relevant

SCAN

Reporting suspected breaches of a Residual Trustee's AML/CFT/CPF obligations

If you suspect a **Residual Trustee may have breached its obligations**, please write to us at this link.

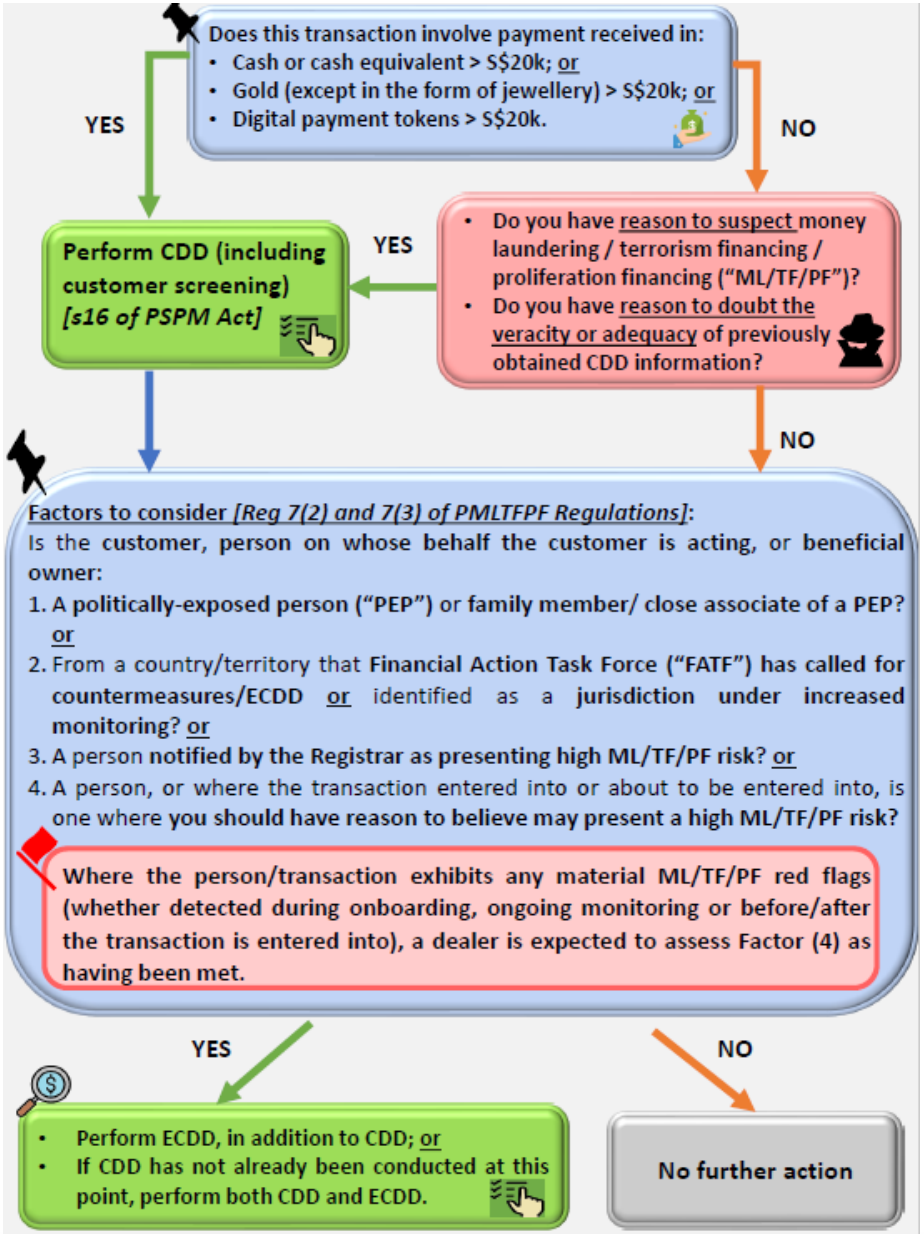
SCAN

Should your concerns **relate to LTCs or PTCs**, please submit the details at this link on the MAS website.

SCAN

CDD and ECDD Obligations

Revised Guide On When To Perform CDD and ECDD Measures



- The revised Guidelines have been updated on MinLaw's website.
- Registered dealers are highly encouraged to download and refer to the latest version.

SCAN

GO.gov.sg

Scan to download the revised Guidelines

When should CDD be performed?

Type and Value of Transaction

- Cash or cash equivalents exceeding $20,000?
- Payment received in gold, other than jewellery (e.g. gold bars) exceeding $20,000?
- Digital payment tokens exceeding $20,000?

Suspicion or doubt about information obtained

- Any reason to suspect ML, TF or PF?
- Any reason to doubt the accuracy or completeness of the CDD information previously obtained?

If answer to either question is “Yes” => Required to conduct CDD regardless of payment mode and value

Factors To Consider When Determining ML, TF and PF Risks

Regulations 7(2) and 7(3) of the PMLTFPF Regulations

PEP or family member or close associate of a PEP

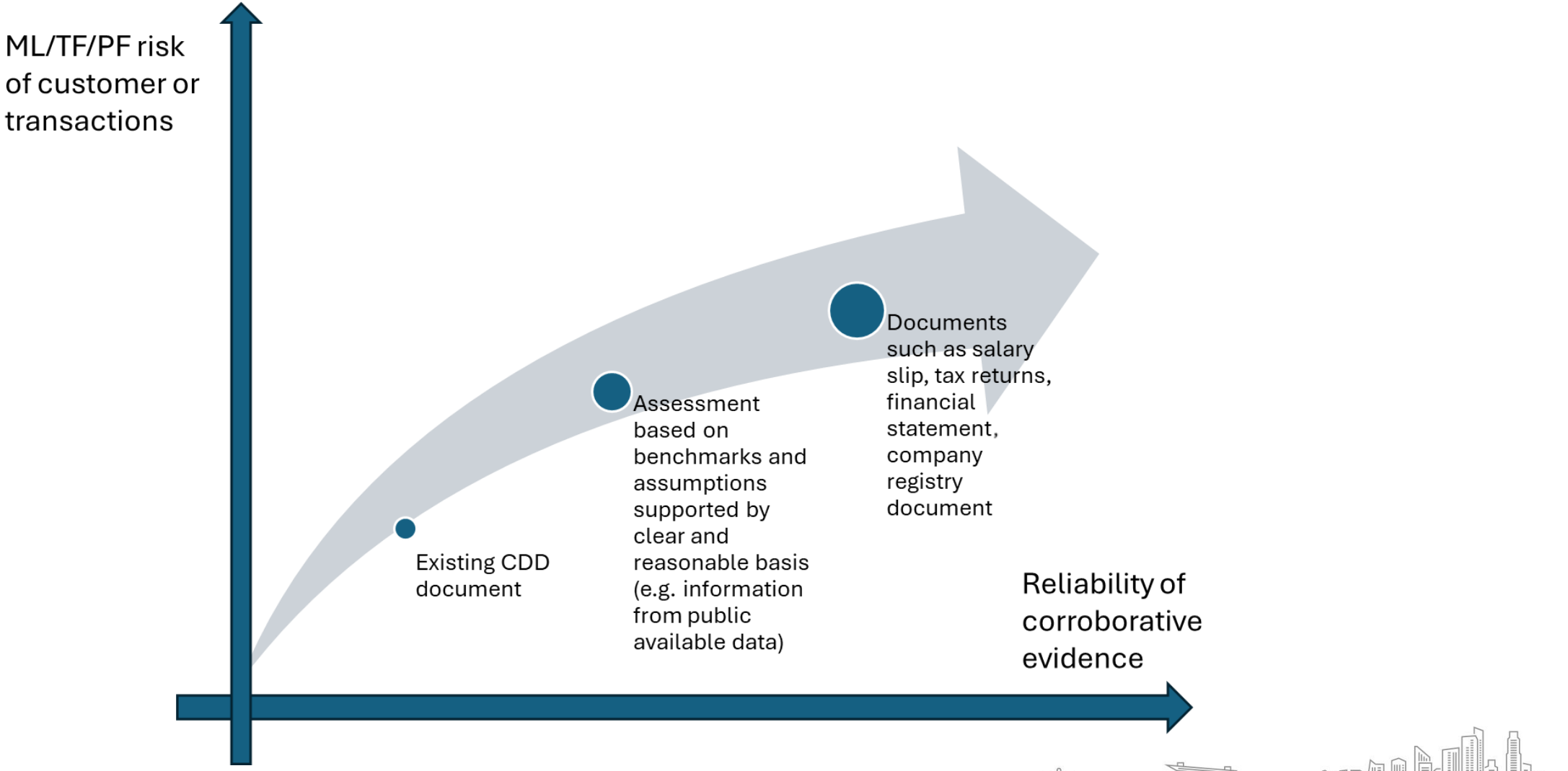
From or connected to jurisdictions identified by the FATF as high-risk or under increased monitoring

Notified by the Registrar as presenting higher ML, TF or PF risks

Any reason to believe that the customer or transaction presents material ML/TF/PF risks

If answer to any of the above is "Yes" => Required to conduct ECDD regardless of payment mode and value. Risk based approach is allowed for ECDD measures conducted.

Adopt Risk Based Approach in Designing SOW checks



Cash Equivalent

Guiding principle
A payment mode would be considered as a cash equivalent if it allows anonymity and the identity of the payer cannot be traced.

Such payment modes would include cash cheques, stored value cards, EZ-link cards, cash vouchers and e-money stored in payment accounts or digital wallets.

Guidelines dated 13 Feb 2026 (Original)
"As a guiding principle, a payment mode would be considered cash equivalent if it allows anonymity and the identity of the payer cannot be traced (e.g. cash cheques, stored value cards, EZ-link cards, cash vouchers, and payment made using digital wallets as mentioned above)."

Guidelines dated 12 May 2026 (Revised)
"As a guiding principle, a payment mode would be considered cash equivalent if it allows anonymity and the identity of the payer cannot be traced (e.g. cash cheques, stored value cards, EZ-link cards, cash vouchers, and ~~payment made using~~ e-money stored in digital wallets as mentioned above)."

Cash Equivalent vs Non-Cash Equivalent

Customer pays using Paynow or Paylah

Not Cash Equivalent

Customer pays using stored value in **Digital Wallet**

Cash Equivalent

Customer pays using **credit or debit card in Digital Wallet**

Not Cash Equivalent

For transactions involving cash equivalent above S$20,000, CDD and CTR requirements have to be complied with.

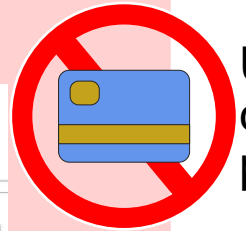
Increased Risk from Contactless Payments…

Scam cases involving bank issued cards

SINGAPORE

Over $1.2m lost to credit card phishing and mobile wallet scams from Oct to Dec 2024

Card Phishing



Unauthorised card provisioning

Fraudulent transactions

Remain alert to red flags indicators

Use of cards in digital wallets that do not belong to the customer

Consider questioning unusual or inconsistent behaviour

File STRs where suspicious circumstances are observed

Source: https://www.straitstimes.com/singapore/courts-crime/over-1-2m-lost-to-credit-card-phishing-and-mobile-wallet-scams-from-oct-to-dec-2024

Suspicious Transaction Report (STR)

When do you file an STR

- Where you **know or have reasonable grounds to suspect** any property represents the proceeds of; was in connection with; or intended to be used in connection with an act which may constitute criminal conduct, and you acquire this knowledge in the course of your profession, you must file an STR

How soon do you need to file an STR

- **As soon as reasonably practicable** upon the establishment of suspicion
- STRs for targeted financial sanctions/ sanctions cases are to be filed **within one business day, if not immediately**
- "As soon as reasonably practicable" should be no longer than 5 business days
- STR filing for higher risk cases should be prioritised

When filing STRs, **select all applicable categories of suspicion**, including anomalies or red-flag indicators, even when adverse news is detected

SCAN

E-file on the Police webpage via STRO Online Notices And Reporting platform (SONAR)

STR Training Videos

SCAN

[About Suspicious Transaction Report]

SCAN

[Red Flag Indicators]

SCAN

[About Suspicious Transaction Reporting Processes]

SCAN

[Encounters with Red Flag Indicators (Part 1)]

SCAN

[Encounters with Red Flag Indicators (Part 2)]

SCAN

[Filing a Suspicious Transaction Report]

Key Takeaways

CDD is not triggered only by transactions thresholds but also by suspicion or doubt.

Once material ML, TF or PF risks are identified, ECDD should be performed regardless of transaction value.

Risk assessment is an ongoing process and not a one-off exercise. Ongoing monitoring of customers and transactions is required.

Regulated entities should keep themselves informed and updated on the latest typologies and relevant red flags.

AML/CFT/CPF Resources

PSMDs

SCAN

Refer to ACD Website for more details – Guidelines for Regulated Dealers

Pawnbrokers

SCAN

Refer to Registry of Pawnbrokers Website for more details – AML/CFT/CPF Resources

Moneylenders

SCAN

Refer to Registry of Moneylenders Website for more details – AML/CFT/CPF Resources

PSMD Enforcement Statistics and Case Studies

Regulatory Supervision and Enforcement

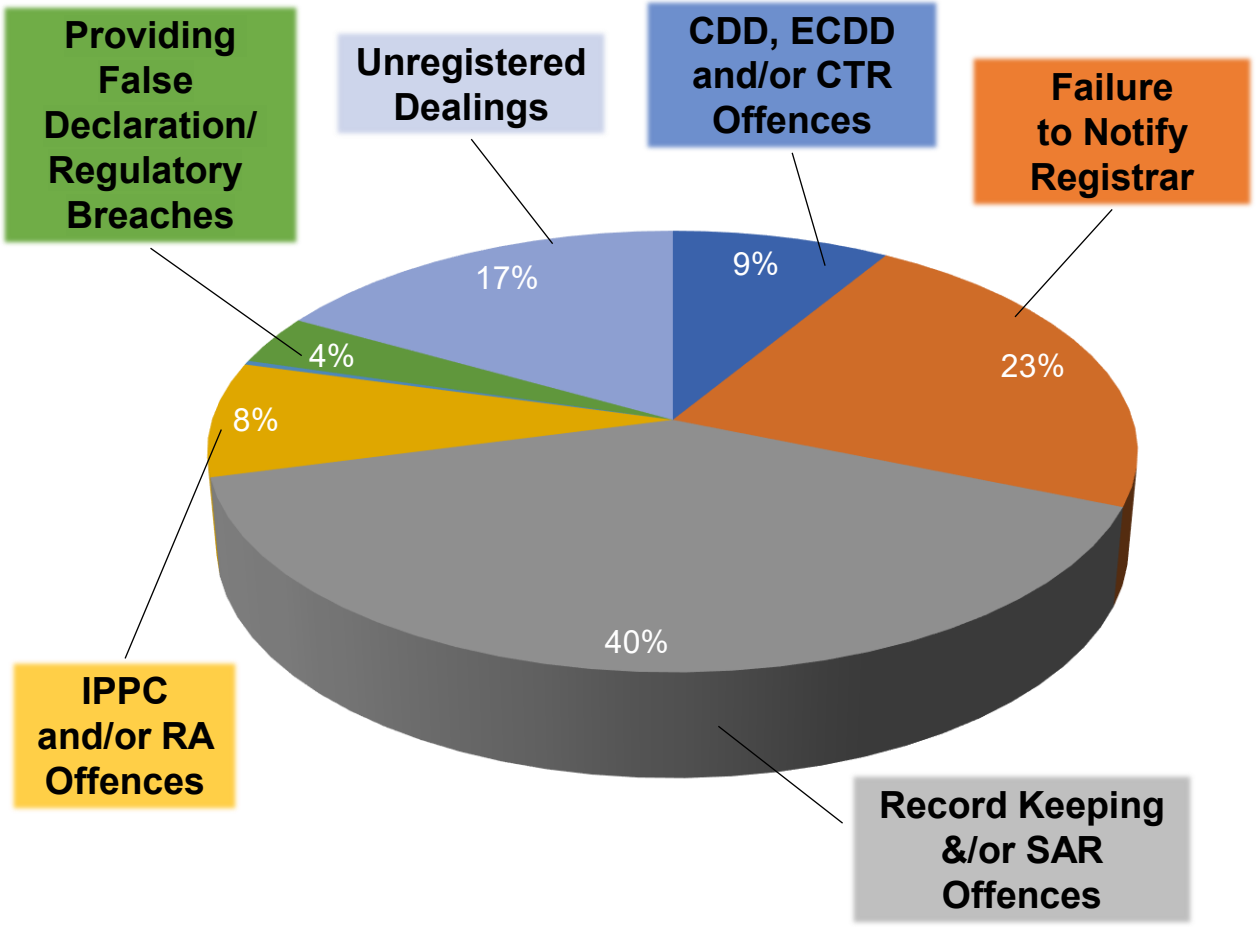
- Supervise PSMD sector for compliance with regulatory requirements
- Deliver fair and effective enforcement outcomes

Two Key Areas of Focus

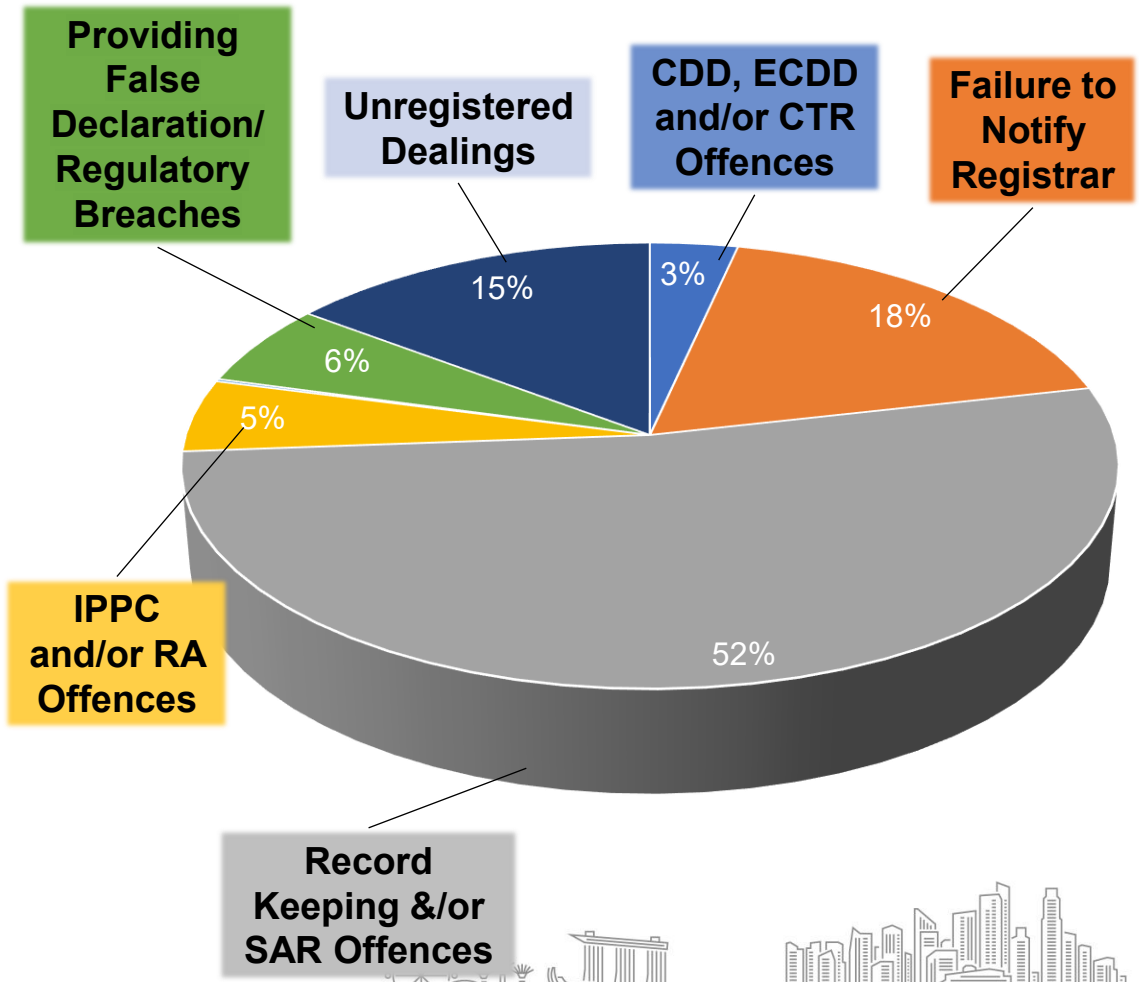
- Non-compliance with AML/CFT/CPF requirements
- Unregistered dealings

Offences

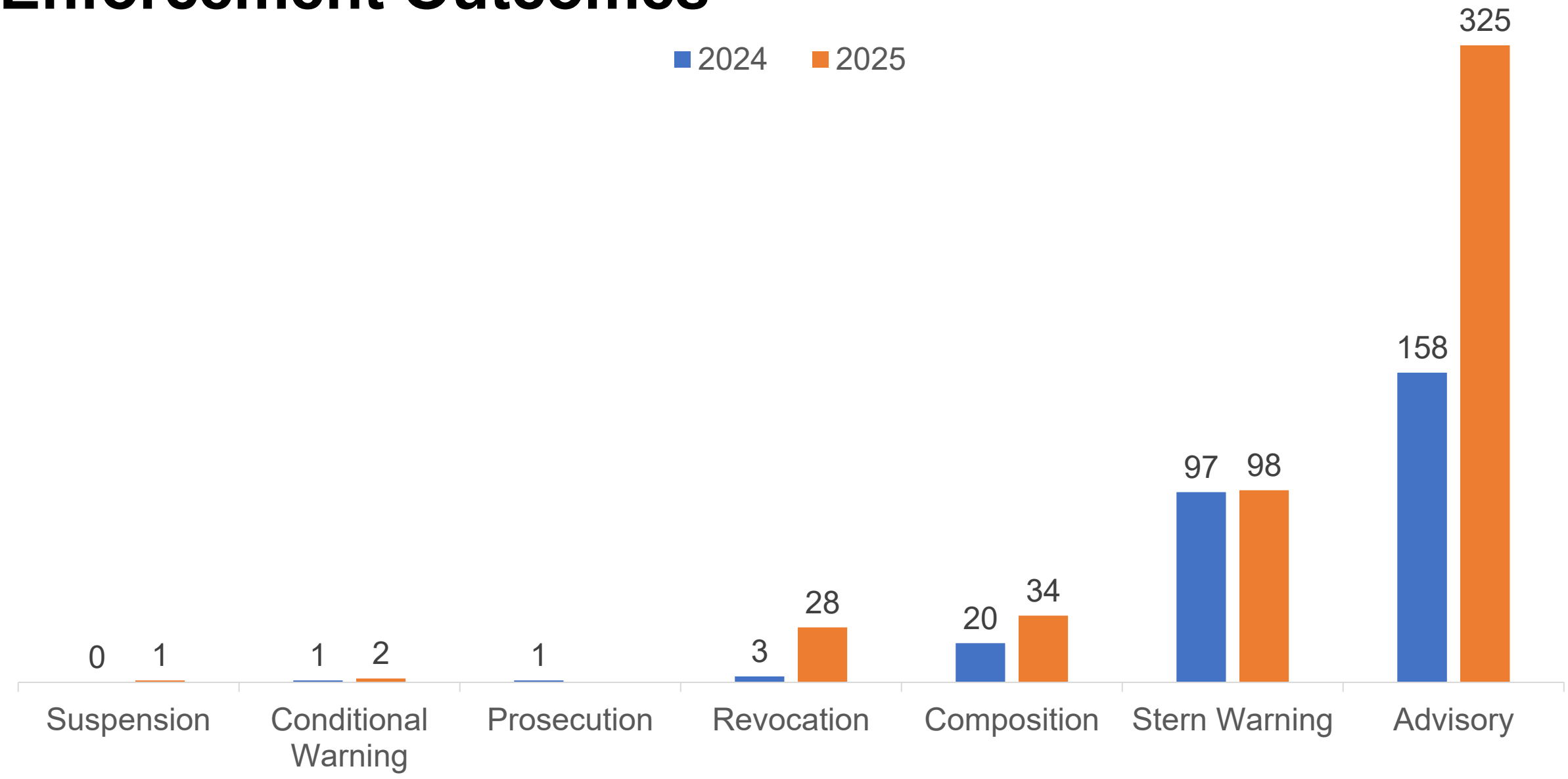
2024



2025



Enforcement Outcomes



CASE STUDY 1: CONDUCTING REGULATED DEALING WITHOUT REGISTRATION

Tip off from a Member of Public

Regulated dealings & sales of precious products (luxury watches, bags and jewellery)

Company A

Selling luxury watches and jewellery dealings since Sep 2023 and was not registered as a regulated dealer

Company B

Selling luxury watches and jewellery dealings since July 2024 and was not registered as a regulated dealer

- Directors of the Company A and Company B were aware of the PSPM Act but continued to sell precious products without a valid registration

FINE

- Conducting unregistered regulated dealing (Sec 6(1) of the PSPM Act), carries a fine of up to $75,000 or imprisonment up to 3 years, or to both.
- In the case of a continuing offence to a further fine not exceeding $7,500 for every day or part of a day during which the offence continues after conviction.

What is Virtual, Digital or Crypto Currency?

- Digital assets existing solely in electronic form
- Not backed or issued by governments or central banks
- Examples include Bitcoin, Ethereum, and stablecoins like USDT
- Used for payments, storing value, or investment
- Transactions recorded on public but pseudonymous blockchains (wallet addresses, not real names)

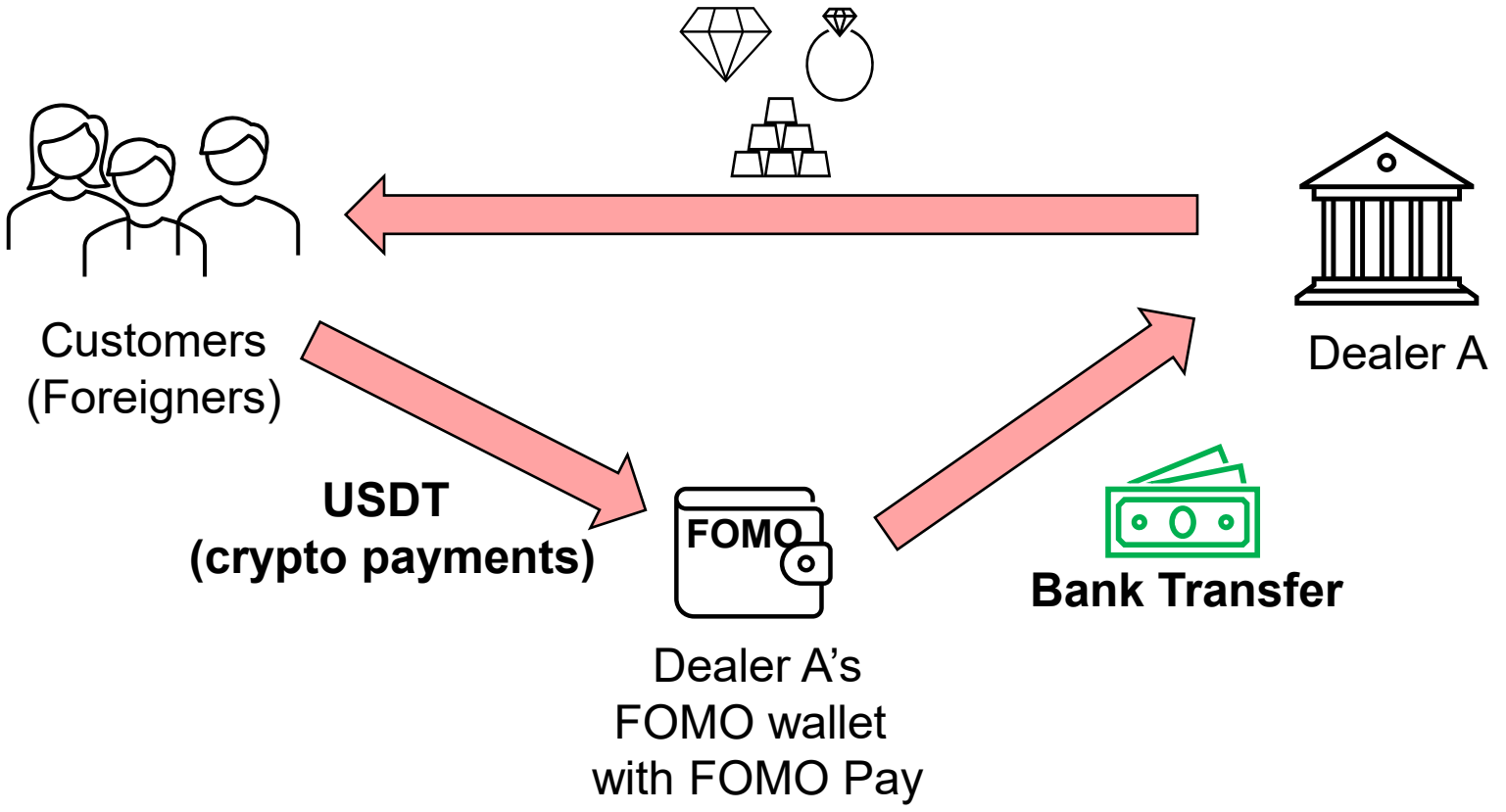
- Crypto is not equivalent to cash or bank transfers
- Where accepted, it poses higher and distinct ML/TF/PF risks that must be actively identified, mitigated and reported

Why Do Crypto Payments Pose Higher ML/TF/PF Risk?

- **Anonymity / pseudonymity**
- **Cross-border by default**
- **Rapid movement of funds**
- **May be linked to illicit activities**

- ✓ CDD requirements on virtual/ digital /crypto payments imposed in Nov 2023
- ✓ Applies to scenarios where virtual/ digital /crypto payments are received through intermediary wallets and converted to funds transferred to regulated entities
- ✓ Crypto-related transactions are high ML/TF/PF risk and ECDD measures have to be applied
- ✓ Before accepting crypto payments, did you
  - Identify and assess the ML/TF/PF risks which may arise?
  - Put in place appropriate measures to mitigate the higher ML/TF/PF risks, e.g. use Transaction Monitoring/ Blockchain Analysis tools to trace the origin of the cryptocurrency? ***(Refer to Reg 15 PMLTFPF Regulations)***

CASE STUDY 2: ACCEPTANCE OF VIRTUAL CURRENCY PAYMENT

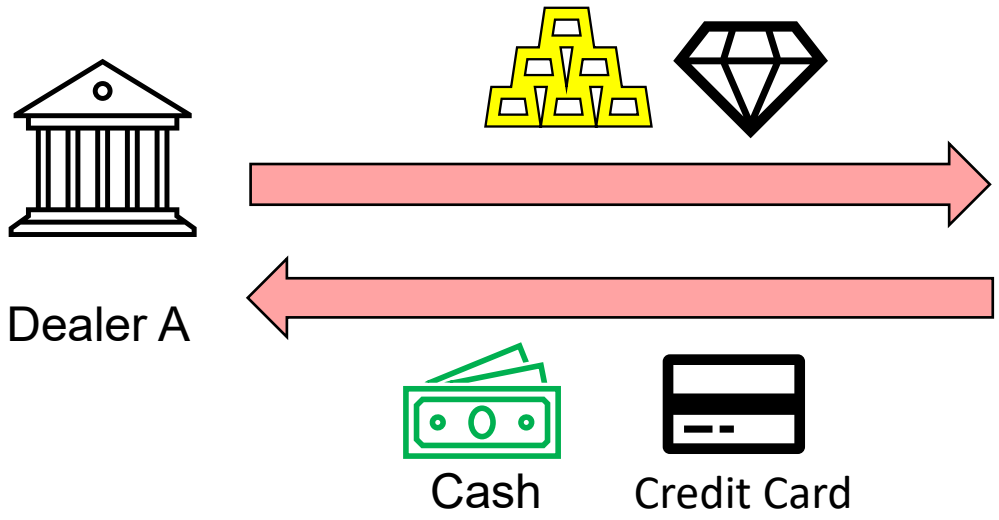


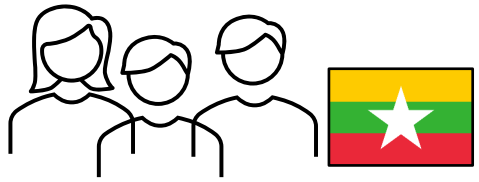
- Transactions were <u>wrongly reported</u> to the Registrar as "electronic payments" instead of reporting them as "crypto currency" payments
- <u>No ECDD measures</u> were conducted on the customers although the customers had paid high amounts in crypto payments

FINE

- Provided false information in SAR (Sec 27(d) of the PSPM Act), which carries a fine up to $50,000 or imprisonment up to 2 years, or to both.
- Failure to conduct ECDD on higher risk transactions involving crypto payments (Reg 7(2)(b) of PMLTFPF Regulations), which carries a fine up to $100,000.

CASE STUDY 3: FAILURE TO CONDUCT ECDD – JURISDICTION SUBJECTED TO A FATF CALL TO APPLY ENHANCED DUE DILIGENCE MEASURES





Customers from jurisdiction subjected to a FATF call to apply enhanced due diligence measures **(Foreigners)**

- No ECDD measures were conducted on the transactions with customers from a jurisdiction subjected to a FATF call to apply enhanced due diligence measures

FINE

- Failure to conduct ECDD on customers from a jurisdiction subjected to a FATF call to apply enhanced due diligence measures [Reg 7(2)(a) of PMLTFPF Regulations], which carries a fine up to $100,000.
- Failure to implement IPPC [Reg 14(1)(c) Of PMLTFPF Regulations], which carries a fine up to $100,000.

Relevant newly prescribed events or circumstances for cancellation of registration under Reg 21(A) of PMLTFPF Regulations wef 20 Dec 2024

- The registered dealer failed to make the Semi-Annual Return record available to the Registrar.
- The registered dealer's Semi-Annual Return made available to the Registrar record no sale of any precious stone, precious metal or precious product.
- The registered dealer has failed to respond to any correspondence sent by the Registrar, where a response is required.
- The registered dealer or its beneficial owners could not be contacted or located after reasonable efforts by the Registrar.
- There is credible information received by the Registrar that the registered dealer is not carrying on the business of regulated dealing or business as an intermediary in Singapore.
- There is lack of proof that the dealer is carrying on business of regulated dealing or business as an intermediary in Singapore.

CASE STUDY 4: CANCELLATION OF PSMD REGISTRATION

(Where there is credible information received by the Registrar that the registered dealer is not carrying on the business of regulated dealing or business as an intermediary in Singapore)

Notice of Intention to Cancel Registration (NICR)

Dealer

Representation by Dealer on why registration should be retained

14 days

Some matters that the Registrar may consider:

- *No representation made to the Registrar within 14 days after service of the NICR*
- *No concrete plans or evidence supporting the commencement of regulated business in Singapore*
- *No information provided to suggest the conduct of a business of regulated dealing or intermediary for regulated dealing in Singapore.*

Businesses may submit a fresh registration application to the Registrar when ready to commence or carry on the business of regulated dealing or business as an intermediary in Singapore.

Sharing by Cyber Security Agency of Singapore

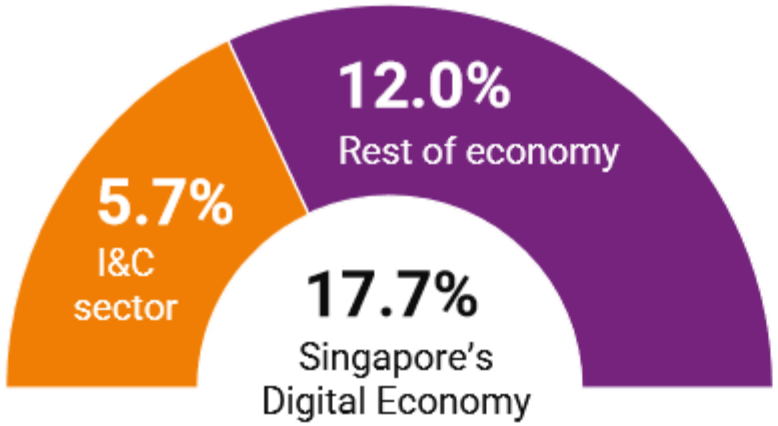
FROM RISK TO RESILIENCE

MAKING CYBERSECURITY YOUR COMPETITIVE ADVANTAGE

Safer Cyberspace Division
Cyber Security Agency of Singapore

The digital economy opens up new opportunities for organisations in Singapore

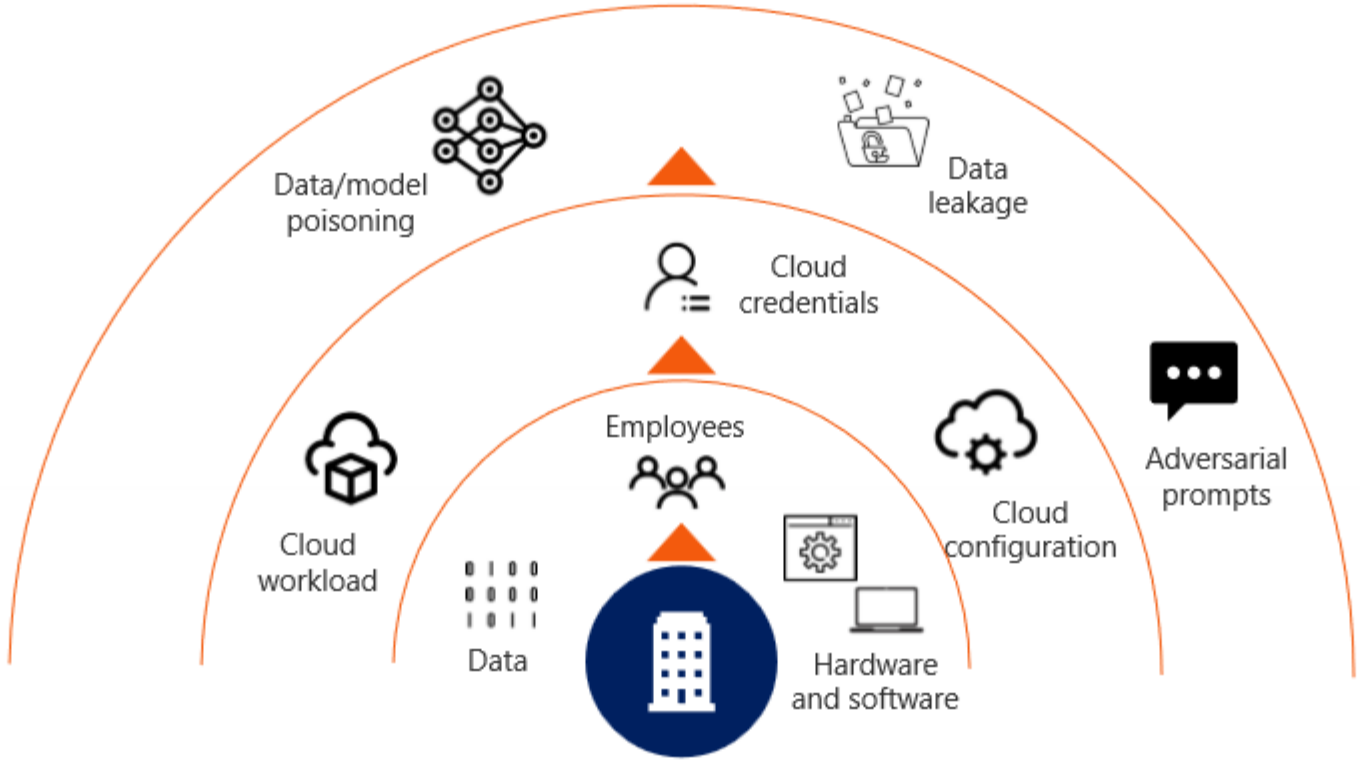
Composition of Singapore's digital economy size (% of GDP), 2023



Digital adoption intensity by sector

Source – IMDA, "Singapore Digital Economy Report 2024"

However, organisations need to implement cybersecurity to manage the expansion of its digital attack surface

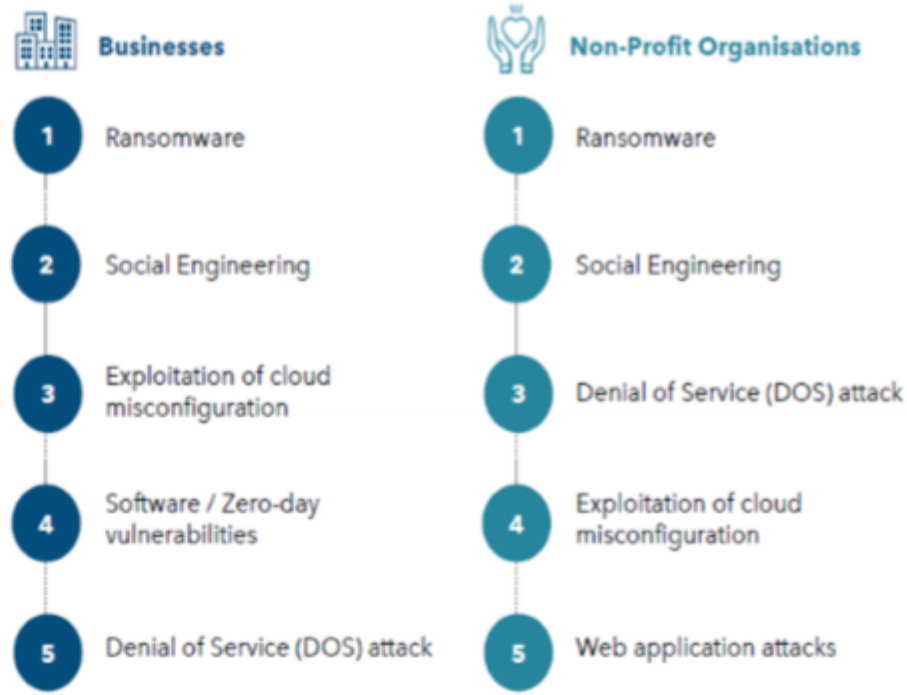


How vulnerable are Singapore organisations to cybersecurity incidents?

Over 8 in 10 have encountered a cybersecurity incident in a year

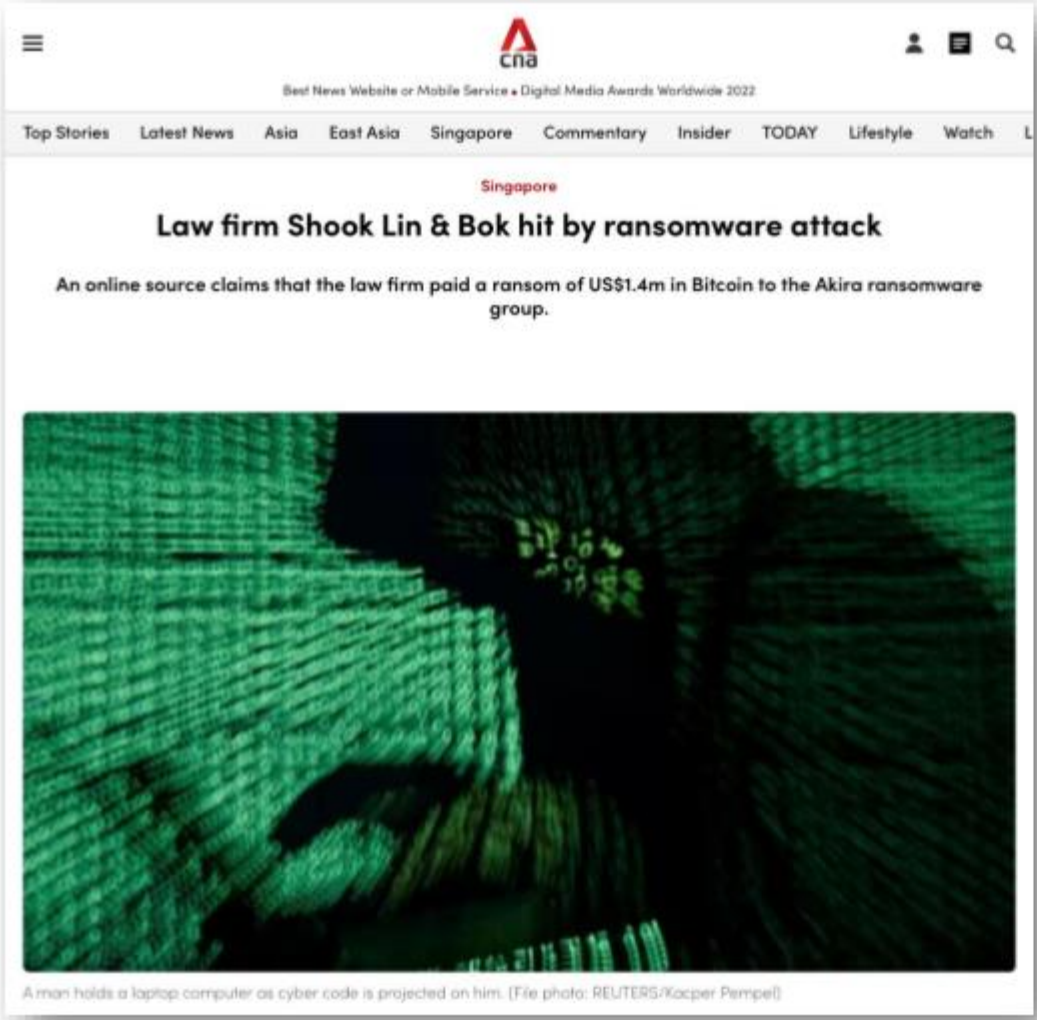
Frequency of Incidents

Top 5 Incidents



Source – CSA, Singapore Cybersecurity Health Report 2023

Examples



May 2024

July 2024

How does cybersecurity incidents impact your organisation?

99% of these organisations suffered a business impact

Businesses

Business Disruption

Data Loss

Reputation Damage

31%	Financial loss
27%	Incident response cost
26%	Regulatory implications

Non-Profit Organisations

Data Loss

Business Disruption

Reputation Damage

34%	Financial loss
25%	IP and/or Trade Secret loss
24%	Incident Response cost

Source – CSA, Singapore Cybersecurity Health Report 2023

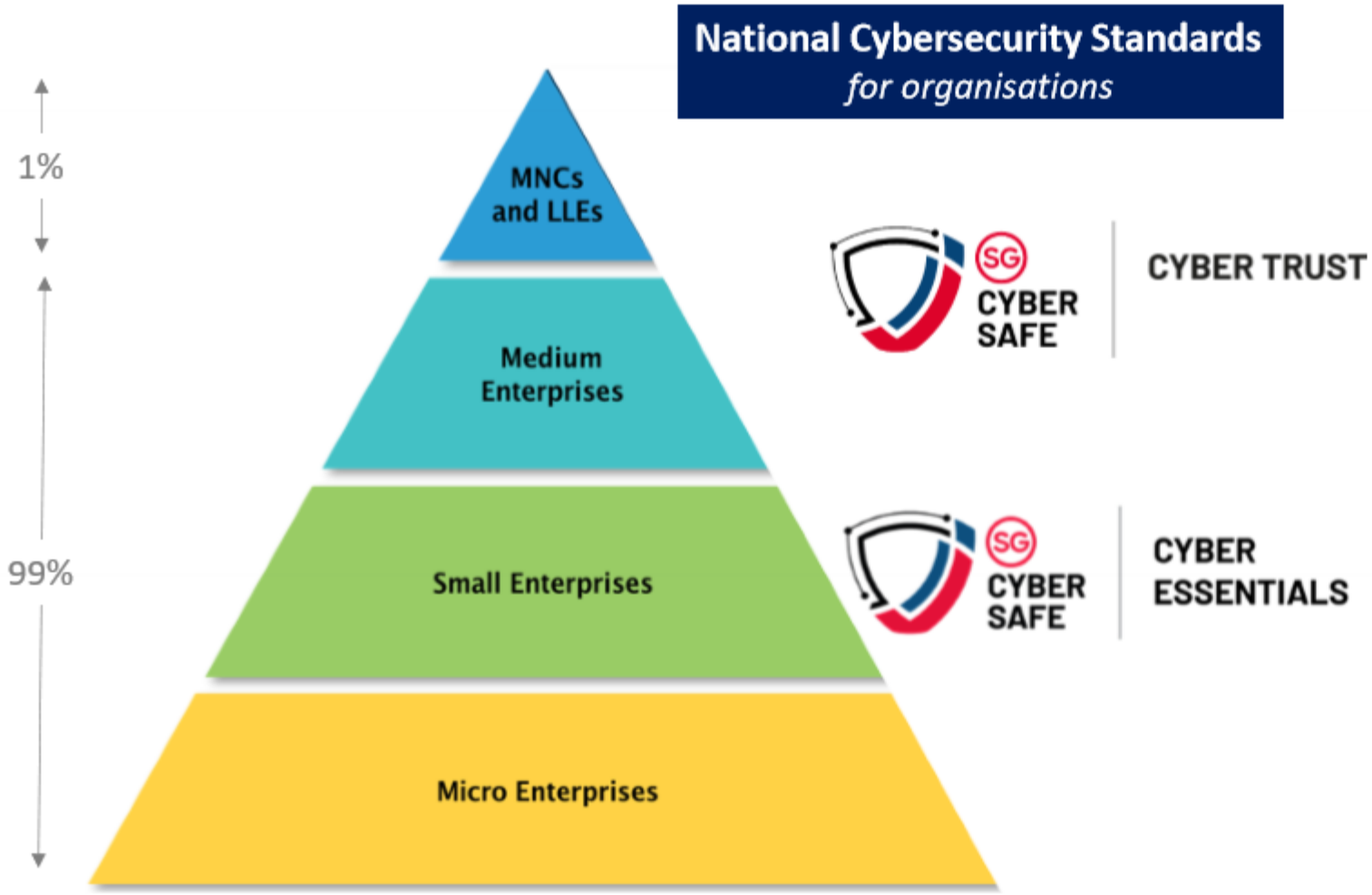
FROM RISK TO RESILIENCE

MAKING CYBERSECURITY YOUR COMPETITIVE ADVANTAGE

1. Overview – How cybersecurity can be your competitive advantage
2. Cyber Essentials and Cyber Trust as cybersecurity 'goals' for the organisation
3. Support available to organisations

CSA SINGAPORE

Cyber Essentials and Cyber Trust as national cybersecurity standards to guide cybersecurity implementation for orgainsations



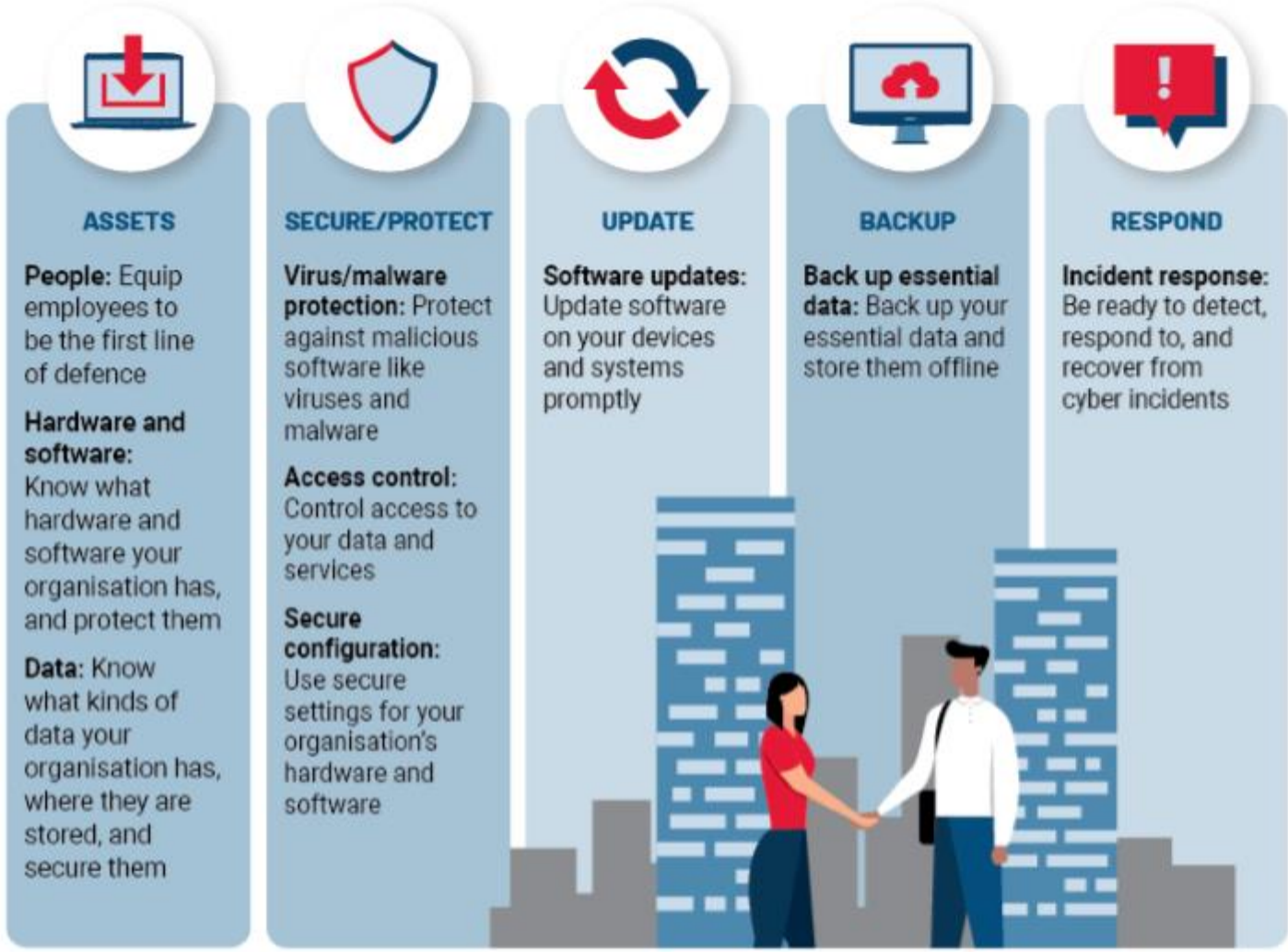
For organisations that have gone beyond cyber hygiene

- Helps organisations take a risk-based approach to cybersecurity
- Provides guided risk assessment for organisations to match their risk level to their cybersecurity implementation

For organisations embarking in cybersecurity

- Helps organisations prioritise the cyber hygiene measures to implement first
- Equips organisations against common cyber attacks

Cyber Essentials provides protection from common cyber attacks



ASSETS

People: Equip employees to be the first line of defence

Hardware and software: Know what hardware and software your organisation has, and protect them

Data: Know what kinds of data your organisation has, where they are stored, and secure them

SECURE/PROTECT

Virus/malware protection: Protect against malicious software like viruses and malware

Access control: Control access to your data and services

Secure configuration: Use secure settings for your organisation's hardware and software

UPDATE

Software updates: Update software on your devices and systems promptly

BACKUP

Back up essential data: Back up your essential data and store them offline

RESPOND

Incident response: Be ready to detect, respond to, and recover from cyber incidents

SG CYBER SAFE | CYBER ESSENTIALS

Certification Validity	**2** years
Assessment Mode *By independent assessor*	Desktop assessment

www.csa.gov.sg/cyber-essentials/

Cyber Trust mark helps organisations to take a risk-based approach to cybersecurity

MARK OF DISTINCTION FOR ORGANISATIONS WITH MORE EXTENSIVE DIGITALISATION

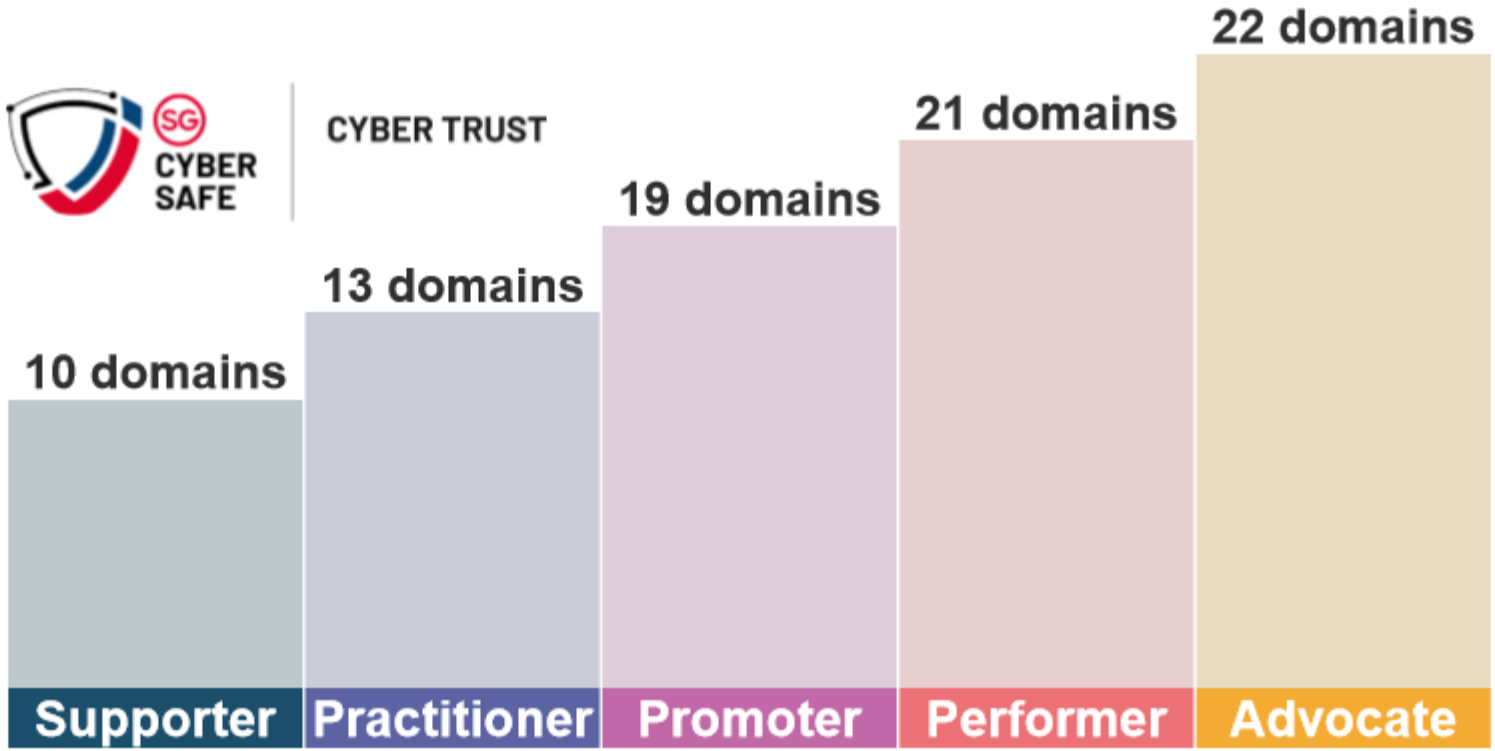
- Recognise organisations as **trusted partners** with robust cybersecurity
- Takes on **risk-based approach** to meet your organisation needs without over-investing

Certification Validity

3 years

Assessment Mode
By independent assessor

1. Documentation
2. Implementation and effectiveness



www.csa.gov.sg/cyber-trust/

Cyber Essentials and Cyber Trust now cover cloud, AI and OT security – Seamless protection for organisations as they undergo digital transformation

Cloud

NEW

Scope –
Cloud setup in orgn

Shared Responsibility Model

Operational Technology (OT)

NEW

Scope –
OT setup in orgn

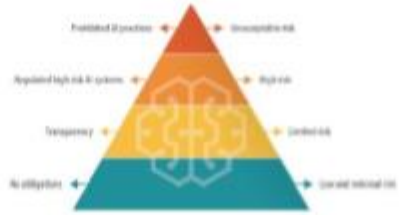
Safety

AI

NEW

Scope –
AI systems in orgn

Safety and AI risk mgmt



. . .

Classical Cybersecurity - Risk-based approach

Scope - Organisation-Level

SG CYBER SAFE | CYBER ESSENTIALS

Cyber hygiene

SG CYBER SAFE | CYBER TRUST

Risk management

FROM RISK TO RESILIENCE

MAKING CYBERSECURITY YOUR COMPETITIVE ADVANTAGE

1. Overview – How cybersecurity can be your competitive advantage
2. Cyber Essentials and Cyber Trust as cybersecurity 'goals' for the organisation
3. Support available to organisations

CSA SINGAPORE

Helping businesses overcome barriers when implementing cybersecurity

Businesses

- **59%** **Lack of knowledge / experience**
- **46%** Unlikely to be a target of cyber attacks
- **39%** **Lack of manpower / resources**
- **38%** Low priority for the organisation
- **36%** Low ROI for the business
- **31%** **Lack of budget**
- **20%** Lack of senior management support
- **7%** None

Non-Profit Organisations

- **56%** **Lack of knowledge / experience**
- **49%** Unlikely to be a target of cyber attacks
- **44%** Low priority for the organisation
- **37%** **Lack of manpower / resources**
- **31%** Low ROI for the business
- **27%** **Lack of budget**
- **19%** Lack of senior management support
- **11%** None

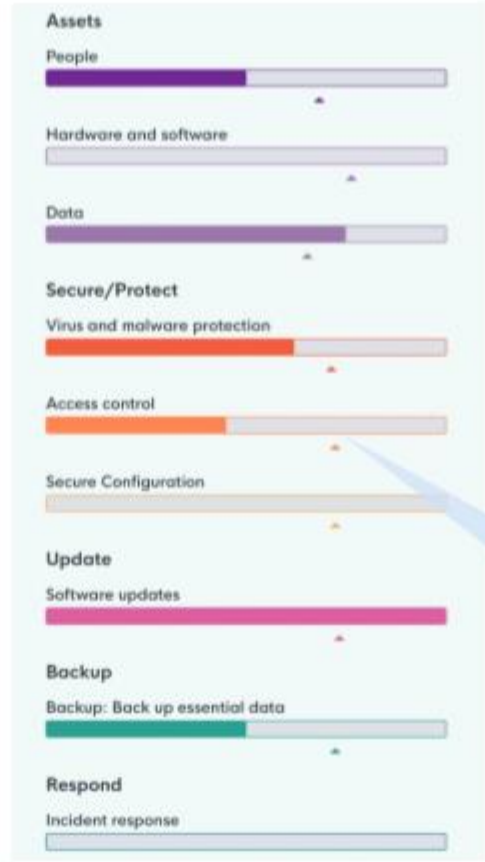
Source – CSA, Singapore Cybersecurity Health Report 2023

Helping organisations overcome barriers in cybersecurity

Cyber health check tool for organisations to measure their cybersecurity implementation

www.csa.gov.sg/cyberhealthchecktool

Personalised score for the organization, versus national average



Score breakdown, versus industry benchmark

Recommendations, e.g.

- Lower scores → CISO–as-a-Service Providers
- Higher scores → Cyber Essentials

Helping organisations overcome barriers in cybersecurity

Cyber self-assessment for organisations to assess readiness prior to appointing certification body

Requirements ("shall" statements)						
total	yes	no	fail	pass	status	result
2	2					Pass
8	8					Pass
4	4					Pass
9	9					Pass
12	11	1				Fail
5	4	1				Fail
1	1					Pass
6	6					Pass
2	2					Pass
49	47	2				Fail

SG CYBER SAFE | CYBER ESSENTIALS

www.csa.gov.sg/cyber-essentials/

Helping organisations overcome barriers in cybersecurity

[1] Guided cybersecurity health plan with consultants onboarded by CSA to help organisations close cyber hygiene gaps

[2] Funding support

www.csa.gov.sg/cybersecurityhealthplan

APPROACH YOUR CHIEF INFORMATION SECURITY OFFICER (CISO)

as-a-Service Consultants

"Cybersecurity health doctor"

DEVELOP YOUR CYBERSECURITY HEALTH PLAN

Up to 70% support [1]

Cyber Health "Checkup"

Preventive Measures

MAKE CYBERSECURITY YOUR COMPETITIVE EDGE

Attain your cybersecurity goals

CYBER ESSENTIALS

CYBER TRUST

1 – For eligible organisations

Helping organisations overcome barriers in cybersecurity

[3] Cybersecurity Health Clinics

Cybersecurity Health Clinics

CISO-as-a-Service (CISOaaS) consultant giving a deep dive into Cyber Essentials

Cyber Essentials in Action

Tabletop game to practice with real-world cyber incident scenarios

SG Cyber Safe programme to help organisations at different stages of their cybersecurity journey

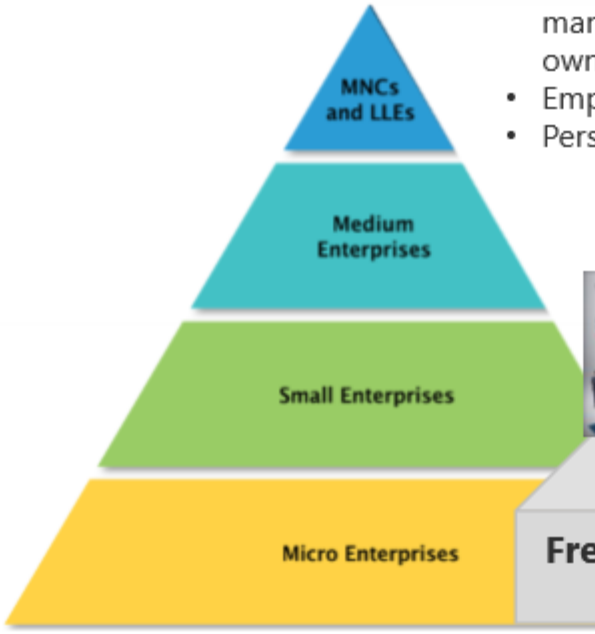
SG CYBER SAFE

Goal

Generate awareness → **Enable action** → **Help orgs attain minimum or appropriate level of cybersecurity** → **Manage digital security risks holistically**

For different roles in organisation:
- Senior management/SME owners
- Employees
- Personnel overseeing IT

Onboard consultants to help orgs with
- Tailored cybersecurity health plans
- Close cyber hygiene gaps
- Funding support



Free cybersecurity toolkits

Cybersecurity consultancy

National Standards

CYBER SAFE | CYBER ESSENTIALS

National Standards

CYBER SAFE | CYBER TRUST

New Technologies

www.csa.gov.sg/sgcybersafe

THANK YOU

www.csa.gov.sg

CSAsingapore

CSA SINGAPORE

Sharing by SPF

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Scam Situation in Singapore & SPF's Anti-Scam Efforts

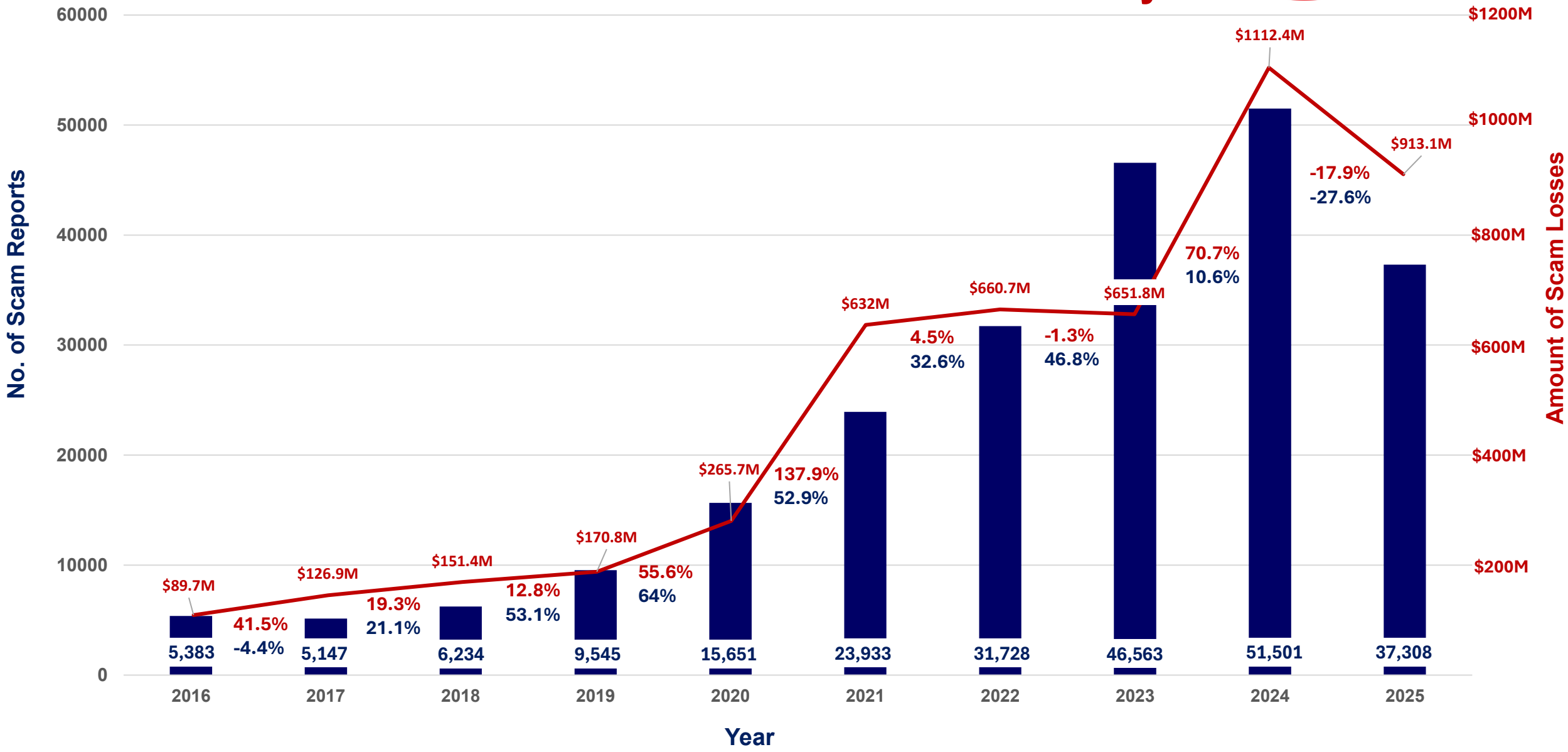
Fighting Scams is a Community Effort

A community is a group of people sharing the same environment. They usually have shared interests.
Fighting scams is a shared responsibility. Everyone plays a part!

Anti-Scam Command
Commercial Affairs Department

Overview of Scam Situation in Singapore

Over $4.7 billion lost to scams in the last 10 years



TOP 10 SCAMS OF CONCERN

	1	2	3	4	5
					
	E-COMMERCE SCAMS	PHISHING SCAMS	JOB SCAMS	INVESTMENT SCAMS	GOVERNMENT OFFICIALS IMPERSONATION SCAMS
TOTAL NUMBER OF CASES REPORTED	6,703	6,264	5,575	5,462	3,363
TOTAL AMOUNT LOST	$16.7 MILLION	$39.9 MILLION	$123.5 MILLION	$336.2 MILLION	$242.9 MILLION
AVERAGE AMOUNT LOST PER CASE	$2,503	$6,384	$22,163	$61,559	$72,229

	6	7	8	9	10
					
	FAKE FRIEND CALL SCAMS	SEXUAL SERVICES SCAMS	INSURANCE SERVICES SCAMS	LOAN SCAMS	INTERNET LOVE SCAMS
TOTAL NUMBER OF CASES REPORTED	1,551	1,150	1,003	935	917
TOTAL AMOUNT LOST	$4.7 MILLION	$3.9 MILLION	$25.2 MILLION	$7.0 MILLION	$24.9 MILLION
AVERAGE AMOUNT LOST PER CASE	$3,056	$3,464	$25,125	$7,515	$27,202

TOP 5 CONTACT METHODS

While social media, messaging platforms and online shopping platforms remained the top contact methods for scammers, there has been a decrease in reported scam cases involving these contact methods.

1	2	3	4	5
				
SOCIAL MEDIA	**MESSAGING PLATFORMS**	**PHONE CALLS**	**ONLINE SHOPPING PLATFORMS**	**OTHER WEBSITES**
2025: 10,448	2025: 9,355	2025: 5,477	2025: 3,804	2025: 2,035
2024: 14,991	2024: 15,145	2024: 6,739	2024: 5,079	2024: 2,056

SCAM VICTIM PROFILE

85.2% of the scam victims were youths, young adults, and adults aged below 65.
The average amount lost per elderly victim was also the highest among the age groups.

Youths

AGES 19 AND BELOW:

E-commerce scams, Phishing scams, Job scams

Young adults

AGES 20 – 29:

E-commerce scams, Job scams, Phishing scams

Adults

AGES 30 – 49:

E-commerce scams, Phishing scams, Job scams

Young seniors

AGES 50 – 64:

Phishing scams, Investment scams, Job scams

Government officials impersonation scams

AGES 65 AND ABOVE:

Investment scams, Government officials impersonation scams, Phishing scams

Formation of Anti-Scam Centre In Singapore

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Singapore's Anti-Scam Strategy – A Collaborative Approach

A Whole-of-Government (WOG) and Whole-of Society Approach to Scam Fighting

Ministry of Home Affairs (MHA)

Secretariat for Inter-Ministry Committee on Scams (IMCS),
which drives and develops WOG policies and initiatives

Securing Communications Infrastructure and Online Space

MINISTRY OF DIGITAL DEVELOPMENT AND INFORMATION
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
CSA SINGAPORE
GOVTECH SINGAPORE

Securing Banking Channels and Government Services

Monetary Authority of Singapore
SMART NATION & DIGITAL GOVERNMENT OFFICE

Enforcement & Recovery

REPABLIK POLIS SINGAPURA

Public Education

MINISTRY OF DIGITAL DEVELOPMENT AND INFORMATION

Scam Public Education Office

Telecommunication Companies

Online Marketplaces & Platforms

Banks, Payment Service Providers, Cryptocurrency Houses & Remittances

DBS · OCBC Bank · UOB · standard chartered · CIMB · HSBC

All Stakeholders

Community Partners

Members of Public

Slide credit to PDD/MHA

Singapore's Anti-Scam Strategy

Scammers' Kill-Chain

Scam Kill Chain is a concept that allows one to understand how scammers penetrate and deceive victims into parting with all their monies

Strategy to Combat Scams

#1: <u>Prevent & Block</u> Scammers' Approach

#2: <u>Detect & Report</u> Scams Occurring

#3: <u>Enforce & Recover</u> When Scams Happen

#4: Educate Public to ACT Against Scams

Enforcement

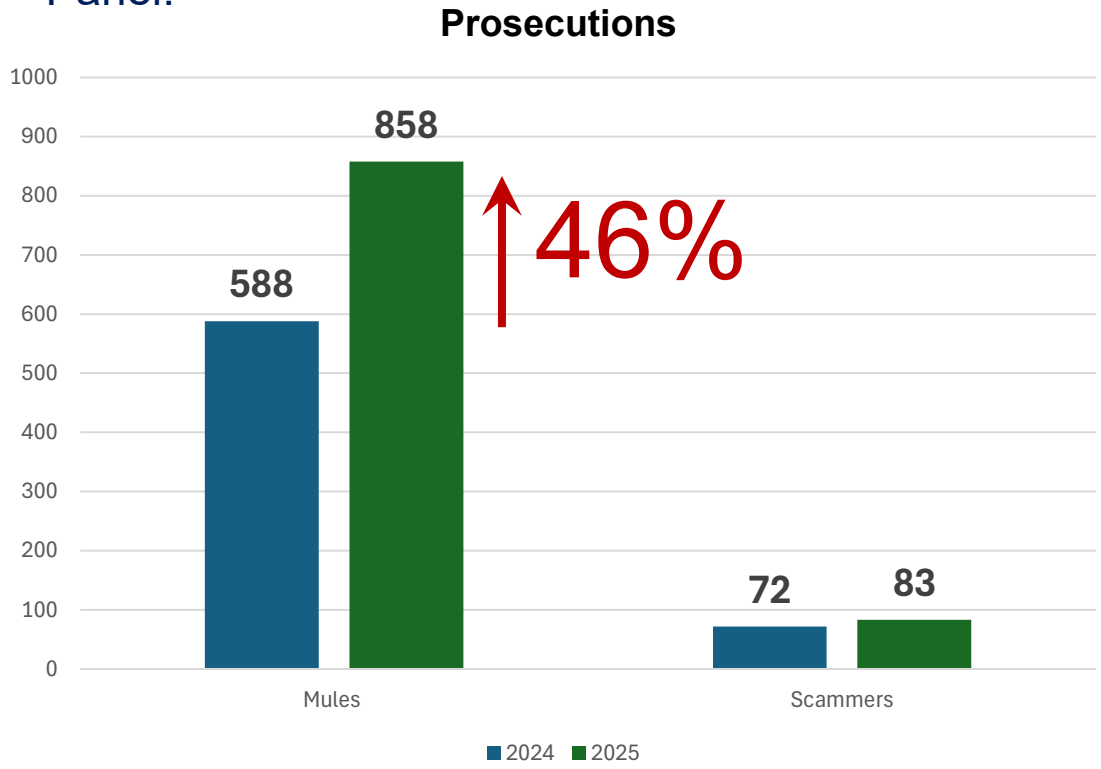
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Policies - Effective policies and robust legislative framework

Singapore's policy interventions and legal framework has made it harder for scammers to operate and enhanced Police's ability to fight scams.

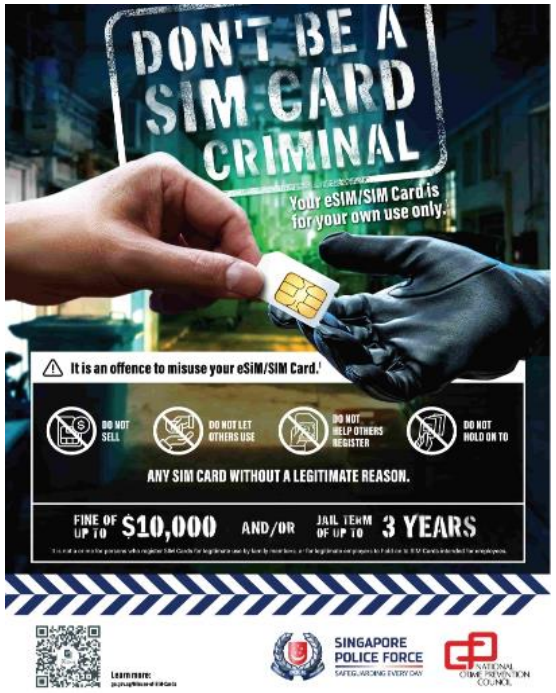
Enhancing Prosecution of Money Mules & Scammers

- Police have pushed for prosecution of mules/scammers, supported by enhanced, deterrent sentencing guidelines from the Sentencing Advisory Panel.



Operationalisation of offence to criminalise the misuse of local SIM cards wef 1 Jan 2025

- Legal changes and close collaboration with IMDA have enabled Police to target SIM card mules and make it more difficult to obtain local SIM cards, a key scam approach vector.



Collaborating with Courts on Mass-Prosecution

41 people to be charged over money mule activities

41 people to be charged over money mule activities

Elaine Lee
Feb 15, 2024 08:48 am

Forty-one people have been arrested for

41人涉嫌不同诈骗案被警方逮捕 年纪最小的只有16岁

THE STRAITS TIMES SINGAPORE

9 men who allegedly gave their bank accounts to criminal syndicates charged with money mule offences

31 people, including 8 teens, charged over suspected scams, money mule offences

Nadine Chua
The Straits Times

UPDATED: Mar 22, 2024, 05:12pm

Follow topic : SINGAPORE COURTS

SINGAPORE - Thirty-one people were hauled to court on March 22 over their suspected involvement in perpetrating various scams and money mule activities.

This group included eight teenagers, the youngest of whom is 17 years old. The oldest among those charged is 67 years old.

The police said on March 21 that they were allegedly involved in scams such as government official impersonation scams, Internet love scams, malware phishing scams, rental scams and China official impersonation scams.

THE STRAITS TIMES GAPORE

Seven men charged over suspected involvement in money mule activities

tnp NEWS SPORTS ENTERTAINMENT LIFESTYLE RACING

SINGAPORE

7 charged with suspected involvement in money mule acts

Seven men were charged in court on Friday with their suspected involvement in various offences connected to money mule activities including cheating, money laundering and facilitating unauthorised access to computer material.

They include Jacky Lim Yi Li, 33, Ho Jia Jin, 29, Zhao Huanhuan, 34, Engku Noor Ziman Noor Azhar, 23, Mohamad Herman Mohamad Ibrahim, 19, and Muhammad Helmi Kamaruddin, 33.

One of them cannot be named as he is 17 years old, and the identities of those under 18 are protected under the Children and Young Persons Act.

In a press release on Friday, the police said the men were suspected to be involved in various scams such as fake friend call investment scams, job, rental and government officials impersonation scams.

Nine to be charged for allegedly passing bank, Singpass details to scammers for money laundering

SINGAPORE - Nine people will be charged on Tuesday for their suspected involvement in money laundering activities linked to a recent spate of phishing scams involving malware-infected apps.

Six adults, aged 19 to 30, and three teenagers, aged 16 to 18, had bank accounts that were used to launder the criminal proceeds from scams.

They had handed over their banking login details or their Singpass credentials to others in exchange for cash or to be used for putative investment opportunities.

THE STRAITS TIMES

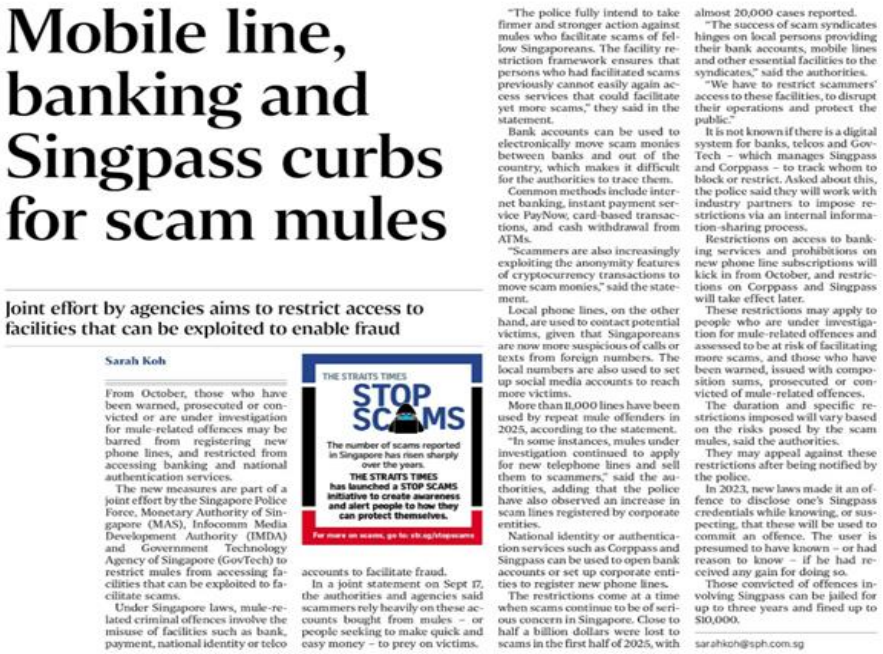
10 suspected money mules, including one teenager, to be charged on Thursday

The suspects allegedly sold or rented their bank accounts to criminal syndicates for as much as $600 per bank account.

Facility Restriction Framework wef 1 Oct 2025

Policy intent is to disrupt scam operations by restricting mules' access to key facilities.

Scam mules should not be allowed to have continued access to new facilities that could be used to perpetrate scams, including bank accounts, digital payment services or mobile lines. Restricting their access to these facilities serves as an upstream, preventive measure to disrupt their ability to facilitate scam operations.



Mobile line, banking and Singpass curbs for scam mules

Joint effort by agencies aims to restrict access to facilities that can be exploited to enable fraud

Sarah Koh

From October, those who have been warned, prosecuted or convicted or are under investigation for mule-related offences may be barred from registering new phone lines, and restricted from accessing banking and national authentication services.

The new measures are part of a joint effort by the Singapore Police Force, Monetary Authority of Singapore (MAS), Infocomm Media Development Authority (IMDA) and Government Technology Agency of Singapore (GovTech) to restrict mules from accessing facilities that can be exploited to facilitate scams.

Under Singapore laws, mule-related criminal offences involve the misuse of facilities such as bank, payment, national identity or telco accounts to facilitate fraud.

In a joint statement on Sept 17, the authorities and agencies said scammers rely heavily on these accounts bought from mules – or people seeking to make quick and easy money – to prey on victims.

"The police fully intend to take firmer and stronger action against mules who facilitate scams of fellow Singaporeans. The facility restriction framework ensures that persons who had facilitated scams previously cannot easily again access services that could facilitate yet more scams," they said in the statement.

Bank accounts can be used to electronically move scam monies between banks and out of the country, which makes it difficult for the authorities to trace them.

Common methods include internet banking, instant payment service PayNow, card-based transactions, and cash withdrawal from ATMs.

"Scammers are also increasingly exploiting the anonymity features of cryptocurrency transactions to move scam monies," said the statement.

Local phone lines, on the other hand, are used to contact potential victims, given that Singaporeans are now more suspicious of calls or texts from foreign numbers. The local numbers are also used to set up social media accounts to reach more victims.

More than 11,000 lines have been used by repeat mule offenders in 2025, according to the statement.

"In some instances, mules under investigation continued to apply for new telephone lines and sell them to scammers," said the authorities, adding that the police have also observed an increase in scam lines registered by corporate entities.

National identity or authentication services such as Corppass and Singpass can be used to open bank accounts or set up corporate entities to register new phone lines.

The restrictions come at a time when scams continue to be of serious concern in Singapore. Close to half a billion dollars were lost to scams in the first half of 2025, with almost 20,000 cases reported.

"The success of scam syndicates hinges on local persons providing their bank accounts, mobile lines and other essential facilities to the syndicates," said the authorities.

"We have to restrict scammers' access to these facilities, to disrupt their operations and protect the public."

It is not known if there is a digital system for banks, telcos and GovTech – which manages Singpass and Corppass – to track whom to block or restrict. Asked about this, the police said they will work with industry partners to impose restrictions via an internal information-sharing process.

Restrictions on access to banking services and prohibitions on new phone line subscriptions will kick in from October, and restrictions on Corppass and Singpass will take effect later.

These restrictions may apply to people who are under investigation for mule-related offences and assessed to be at risk of facilitating more scams, and those who have been warned, issued with composition sums, prosecuted or convicted of mule-related offences.

The duration and specific restrictions imposed will vary based on the risks posed by the scam mules, said the authorities.

They may appeal against these restrictions after being notified by the police.

In 2023, new laws made it an offence to disclose one's Singpass credentials while knowing, or suspecting, that these will be used to commit an offence. The user is presumed to have known – or had reason to know – if he had received any gain for doing so.

Those convicted of offences involving Singpass can be jailed for up to three years and fined up to $10,000.

sarahkoh@sph.com.sg

THE STRAITS TIMES
STOP SCAMS
The number of scams reported in Singapore has risen sharply over the years.
THE STRAITS TIMES has launched a STOP SCAMS initiative to create awareness and alert people to how they can protect themselves.
For more on scams, go to: str.sg/stopscams

	Phase 1 (From 1 Oct 2025)		Phase 2 (Q1 2026)
	Money Mules	Telco Mules	SingPass Mules
Offences in scope	ss 50, 51, 53, 54, 55, 55A CDSA	• Subscriber: ss 39B(1), 39C(1) MOA • Retailers: ss 39D(1)/(2), 39E, 39F, 39G(1) MOA	ss 8A(1), 8B(1) CMA
Persons in scope	• High-risk mules **under investigation** for scam-related offence(s) *(elaborated in the next slide)* • Mules charged and **undergoing prosecution** for scam-related offence(s) • Mules **warned** of scam-related offence(s) • Mules issued with **composition** for scam-related offence(s) • Mules **convicted** of scam-related offence(s) *Note: All persons in scope will face the same restrictions in the sector of offending conduct.*		
Period of restrictions	• **High-risk mules under investigation**: until case outcome is determined, with yearly reviews by SPF. • **Mules undergoing prosecution**: until case outcome is determined, with yearly reviews by SPF. • **Warned mules, mules issued with composition and convicted mules**: one year from date of warning, payment of composition, or conviction. • **Repeat mules**: Three years for second or more-time offender.		

Caning for Scams and Scams-related Offences

Caning was introduced to deter and punish those who commit scams or facilitate the commission of scams. Scammers, syndicate members and recruiters will face mandatory caning, while scam mules may be subjected to discretionary caning.

Offender Category	Legislative Provisions	Caning Liability
Scammers, Members & Recruiters of Scam Syndicates	• Sec 420(2) PC • Sec 5 & 6 OCA	Mandatory caning of not less than 6 strokes, but not more than 24 strokes.
Scam Mules	• Sec 8A & 8B CMA • Sec 51 & 54 CDSA • Sec 39B, 39C, 39D, 39F & 39G MOA	Discretionary caning of not more than 12 strokes.

These new provisions are applicable to offences committed **on or after** 30 December 2025.

Intervention

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

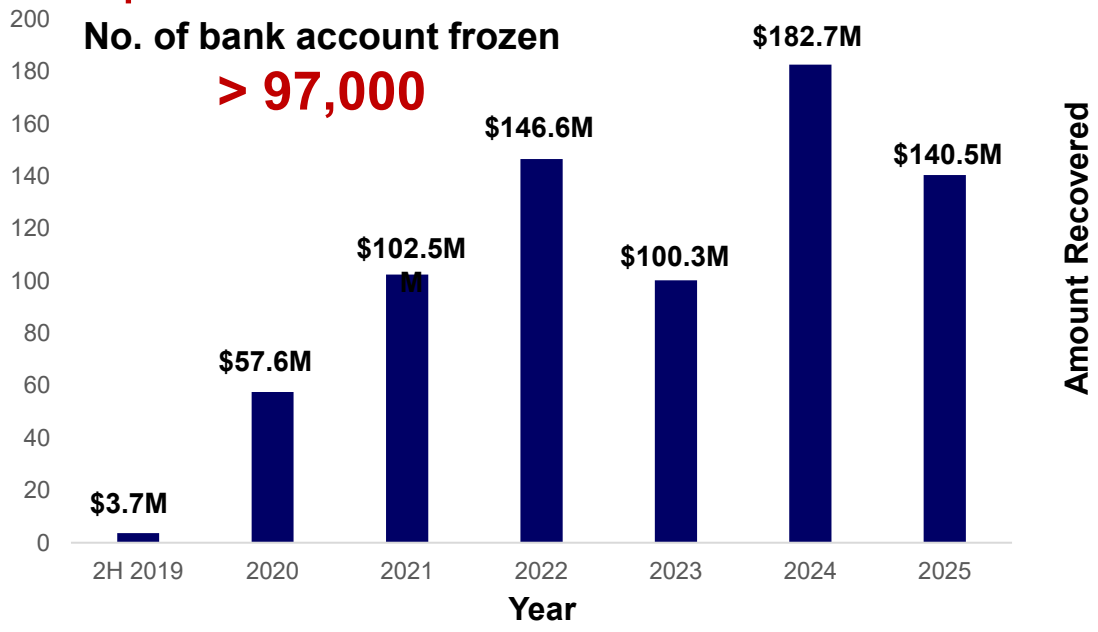
Disruption - Disruptions to deny scammers of operating space

Total Amount Recovered

$734 million

No. of bank account frozen

> 97,000



Swift Account Freezing & Fund Recovery

Period: 1 Jan 2025 – 31 Dec 2025

	Fiat	Crypto	Total
Losses	$730.9M	$182.2M	$913.2M (Fiat Losses + Crypto Losses)
Recovery	$117.7M	$22.8M	$140.5M (Fiat Recovery + Crypto Recovery)
Net Scam Losses	$613.7M (Fiat Scam Losses – Fiat Recovery)	$159.4M (Crypto Scam Losses – Crypto Recovery)	$773.1M (Total Scam Losses – Total Recovery)

DBS · OCBC Bank · UOB · GXS · standard chartered · CIMB · HSBC

Seven Co-located Banks

Key Intervention Approaches

BANKS

Frozen over 97,000 **bank** accounts & recovered more than **$734M**.

MARKETPLACES

Removed more than **94,800** suspicious online monikers & advertisements.

Freezing of bank accounts

Termination of mobile and WhatsApp lines

Removal of monikers & suspicious advertisement

Blocking of websites

June 2019 – 2025
Websites: Since Feb 2024

TELCOS

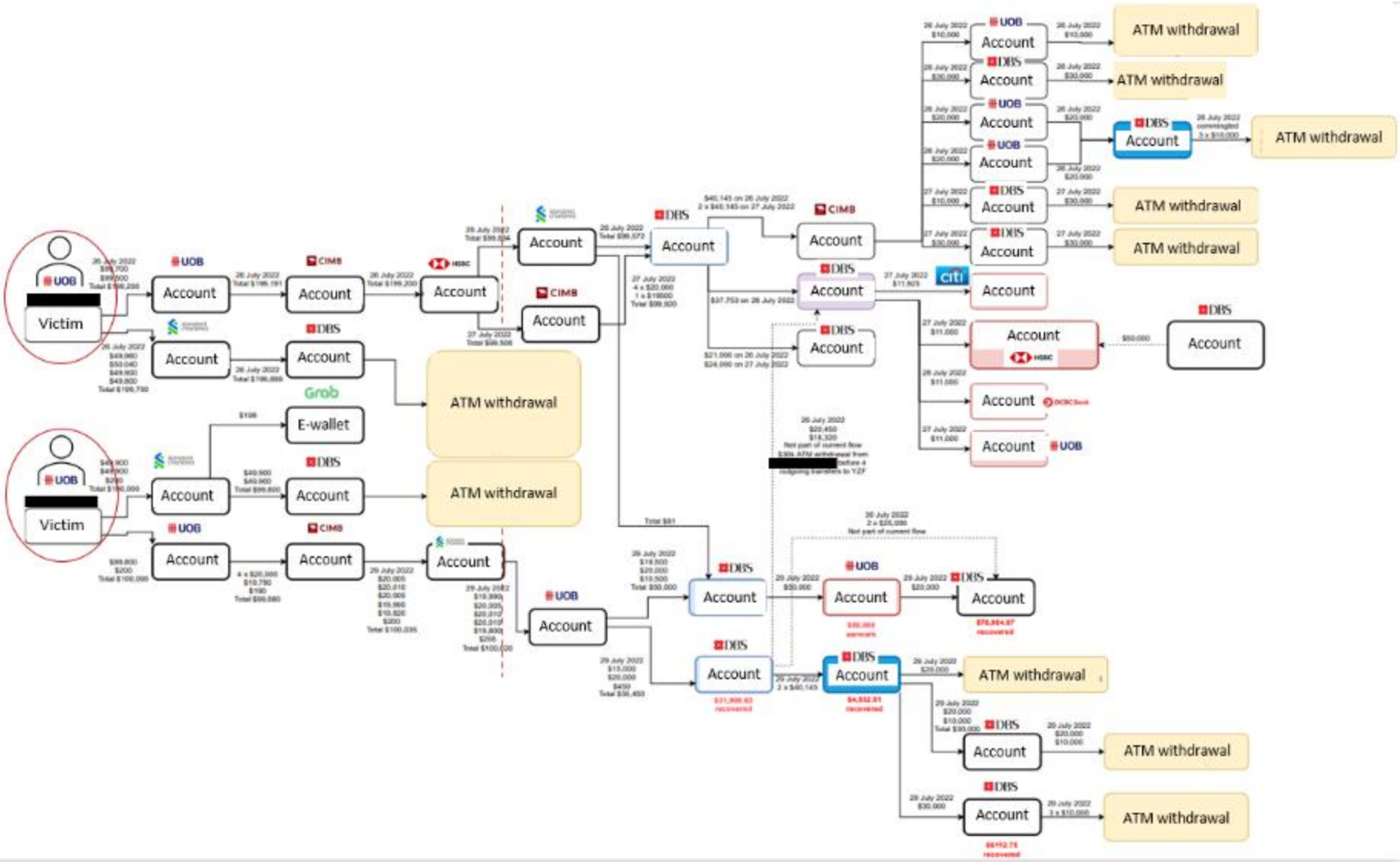
Terminated more than **181,600** mobile lines & reported more than **212,200** WhatsApp accounts.

WEBSITES

Blocked **over 121,100 scam sites**.

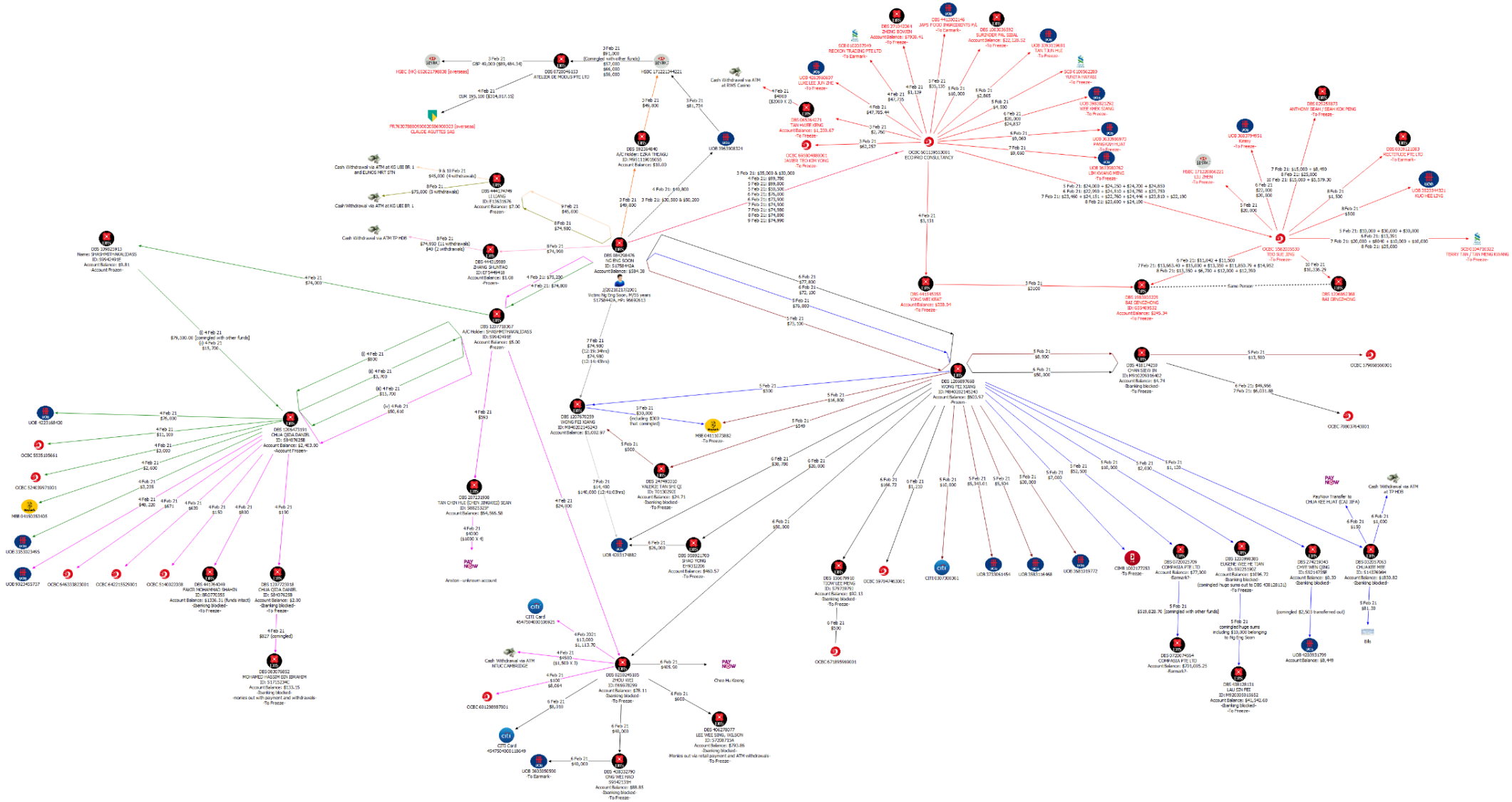
Example of fund-tracing done by ASC

Two cases of Government Official Impersonation Scam involving losses ~S$600,000



Example of an extensive fund tracing carried out by ASC

An overview of an extensive intervention linked to COIS conducted by ASC leading to 89 bank accounts being frozen in a single day



How can the Precious Stone Metal Dealers be involved ?

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Scammers pivoting to gold bars, jewelry and watches

Scammers pivoting to gold bars, jewelry and watches

- Customers making unusually large gold purchases (e.g. jewellery, luxury watches)
- Customers appearing distressed or receiving phone calls while making purchases
- Customers refusing to provide information on the reason for the purchases
- Customers appearing to be in a hurry to complete the transactions
- Verifying the cardholder's name against CDD information
- Observing customer reactions to additional requests for any unusual behaviour

- **File STR**
- **Lodge Police Report**
- **Crime in progress, CALL 999**

Collaborating with National Crime Prevention Council

“I Can ACT Against SCAMS” National Campaign

ADD **Hardware, software, and security settings**

ScamShield	Download ScamShield or other legitimate scam blocking apps.
Privacy settings in social media accounts	Limit and/or prohibit others from viewing your activities or contacting you on social media accounts (e.g., Telegram, Facebook, Instagram, TikTok, LinkedIn).
2-factor / Multi-factor authentication	Set up additional authentication methods for social media, bank or other important online accounts.

CHECK **Taking time to spot scam signs, checking with trusted others, and reconsidering decisions and actions before sharing any money or private information**

Platforms / Parties	Check transaction is done via authentic platforms and with legitimate parties.
With Official Sources and Trusted Others	Check scam signs and trends with legitimate sources (e.g., Singapore Police Force, Scam Alert, Cyber Security Agency of Singapore & National Crime Prevention Council online channels). Also check with trusted others to gain second opinions.
Self (Behaviour/ Emotional State)	Delay responding to requests, orders, or instructions that makes you feel pressured or uncertain.

TELL **Informing authorities and communities about scam encounters, scam signs and trends**

Authorities	Immediately tell authorities (e.g. banks, platforms, the Police etc.) after encountering or falling prey to scams.
Social Circles	Tell individuals in social circles about scam signs, trends, and encounters.

‘I Can ACT (Add, Check, Tell) Against Scams’ Campaign launch on 18 January 2023 at **SCAMINAR**!

ScamShield Suite

- ScamShield has expanded from an app to a **suite of four anti-scam resources** which aims to enable members of the public to better protect themselves against scams:
  - **24/7 ScamShield Helpline 1799**
    - Call to check if you are unsure if something is a scam
  - **Enhanced ScamShield app**
    - Block scam calls and detect scam SMSes
    - Check if something is a scam
    - Share scam encounters with authorities
  - **ScamShield website: www.scamshield.gov.sg**
    - One-stop portal on scams
    - Learn about latest scam trends and protective measures
  - **ScamShield Alert channels**
    - Receive latest information on scams and protective actions

Thank you

SINGAPORE POLICE FORCE

SAFEGUARDING EVERY DAY

Code of Practice

AML Measures to Combat Scams

Ministry of Law

Code of Practice issued on 2 April 2026

AML Measures to Combat Scams-related ML cases

- Scam Typologies involving precious metals, jewellery, luxury watches
- Equip PSMDs with knowledge of red flags
- Establish clear response measures where there are suspicious activities

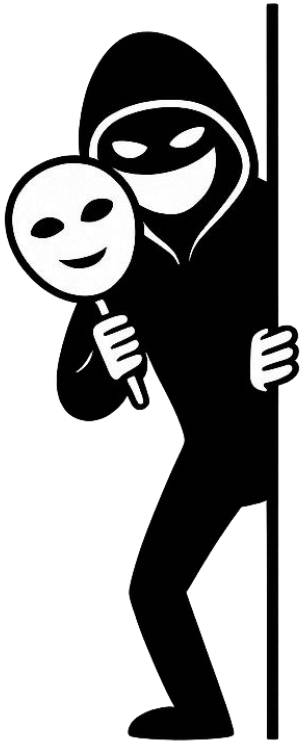
SCAN HERE

https://go.gov.sg/psmd-cop

Code of Practice to combat scam-related ML cases

Scam Typologies – Use of Money Mules

- **Recruitment**: Masterminds recruit Money Mules through modes that include messaging platforms, such as Telegram
- **Transaction Pattern:** Money Mules instructed to
  - purchase gold bars, gold jewellery, luxury watches using cash, bank transfers, PayNow, or credit cards which are funded by scam proceeds
  - Sell them and move the sales proceeds or cryptocurrencies overseas or pass the purchased items to another person
- **Behaviour**: Often appear anxious, stay on phone calls, and make hurried purchases without regard to value/price
- **Other signs**: Other individuals waiting outside the shop while Money Mules conduct the transactions



Scam Typologies – Manipulated Victims

- **Unsolicited Calls**: Victims received unsolicited calls regarding unauthorized transactions
- **Threats**: Calls transferred to purported government officials from police, MAS, Minlaw etc. Victims alleged to be involved in crime or money laundering activities and threatened with arrest or investigation if not cooperative. Victims convinced that they are assisting with legitimate investigation.
- **Transaction Pattern:** Victims instructed to
  - purchase gold bars, gold jewellery, luxury watches using cash, bank transfers, PayNow, or credit cards which are funded by scam proceeds
  - pass the purchased items to another person
- **Behaviour**: Appearing anxious, distressed or taking instructions from others, making hurried large purchases, may visit same retailers on consecutive days, insisting purchases are legitimate and necessary

Scam Red Flags

- Unusually Large Purchases (Above S$20,000)
- Appearing Hurried to Complete Transactions
- No Consideration Of Purchases (Price, Value, Design)
- Repeated High-value Purchases Within A Few Days
- Requesting Split Payments Across Multiple Cards
- Refusing To Provide Reasons or Providing Scripted Reasons
- Unfamiliar with items being bought
- Agitated, Distressed When Questioned

PLEASE NOTE

- **If Scam Red Flags observed, customers/ transactions should be treated as high risk.**
- **CDD and ECDD measures should be conducted.**

A.C.T. Framework

Transactions Above S$20,000 regardless of payment mode

Add	• **Immediate intervention** - ask reasons for purchase
Check	• **Customer behaviour** using anti-scam information (Annex A of COP)
Tell	• **If customer still insistently wants to proceed despite repeated warnings, please call ScamShield Helpline (1799) or 999**

SCAN HERE

Scam Alert Questionnaire

Steps to Take When Red Flags Observed

- Conduct Enhanced Customer Due Diligence (ECDD)
- Seek Family Member Verification Through Phone
- Provide Anti-scam Educational Materials
- Request Customer to Contact ScamShield Helpline
- File Suspicious Transaction Report (STR)
- Escalate to Supervisor and Document Behaviour

- **If customer still insistently wants to proceed despite repeated warnings, please call Scamshield Helpline (1799) or 999.**

Thank you!

@minlawsg