



# MinLaw Industry Compliance and Engagement (MICE) 2025

30 May 2025

- 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.

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.

# Programme

## Audience poll

### Segment 1:

- ACD's Objectives and Principles of Regulatory Oversight
- National AML/CFT/CPF Publications
  - ML NRA and National AML Strategy
  - PF NRA and CPF Strategy
  - VARA
- MHA's Sharing
  - TF NRA and Strategy for CFT
  - Targeted Financial Sanctions Pursuant to TF



# 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:

- Additional Guidance on:
  - Assessment of Customer Risk
  - Identification of Material Red Flags
  - SOW Corroboration
  - Ongoing Monitoring of Customers and Transactions
  - STR Filing Timelines
- Enforcement
- Case Studies (Typologies)

## Kahoot! Quiz



# 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:

- Data Protection – Your Role and Responsibility
- Registration Matters and Resources Available

## Audience Poll

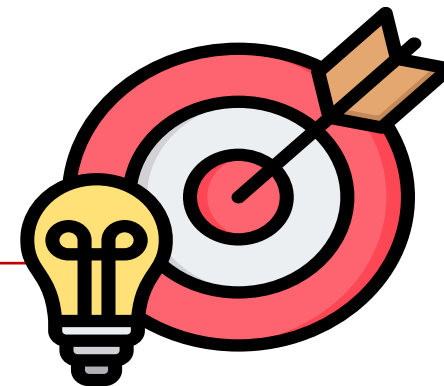
## Q&A



# ACD's Objectives and Principles of Regulatory Oversight



# ACD's Mission and Objectives



## Mission

- To **work with** the regulated community and stakeholders to **protect** the integrity of the financial system and the broader economy from threats of ML/TF/PF.

## Objectives

1. Prevent regulated sectors from being used as conduits to launder criminal proceeds and funds to finance terrorism and proliferation of weapons of mass destruction (WMD).
2. Raise the regulated sectors' awareness and capabilities for timely detection of illicit funds.
3. Take effective enforcement actions to deter regulatory infractions.



Refer to [ACD Website](#) for more details – Notices from the Registrar



# ACD's Regulatory Oversight Functions

## Regulation

- Formulate policies and levers aligned with latest FATF's international standards and tailored to domestic risks
- Lead strategic regulatory development and manage partnerships and engagement

## Authorisation

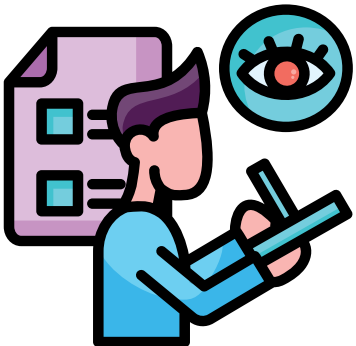
- Assess whether PSMD applicants meet the fit and proper criteria for registration and renewal
- Refuse to grant/renew or suspend/cancel registrations if there are justifiable grounds to do so

## Supervision

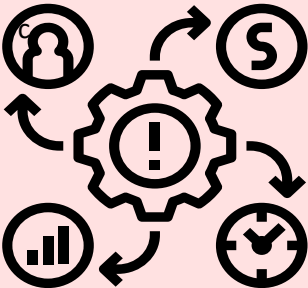
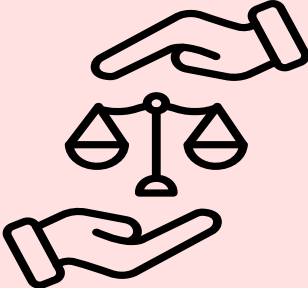


- Supervise and monitor the regulated sectors for AML/CFT/CPF compliance
- Conduct environmental surveillance and targeted risk-based inspections

## Enforcement

- Investigate and act against regulated entities and individuals who breach AML/CFT/CPF requirements



# ACD's Supervisory Principles

Risk-Focused	Impact Sensitive	Supportive of Enterprise	Shared Responsibility
<ul style="list-style-type: none"><li>• Supervision approach based on ML/TF/PF risks</li><li>• Calibrate supervisory response based on risk profiles</li></ul> 	<ul style="list-style-type: none"><li>• Reduce risk and impact of failures</li><li>• Proportionate action in line with the desired regulatory objectives and outcomes</li><li>• Provide transparency and regulatory certainty</li></ul> 	<ul style="list-style-type: none"><li>• Supervise without undue compliance burden</li><li>• Consultative approach to achieve desired regulatory outcomes</li></ul> 	<ul style="list-style-type: none"><li>• Shared ownership of regulatory objectives and outcomes</li><li>• Partnership approach with industry and stakeholders</li></ul> 





# National AML/CFT/CPF Publications in 2024/2025



# Singapore's ML/TF/PF Risk Profile



Singapore is an international financial centre / business and trading hub

- **Exposure to cross-border asset and fund flows** – raises risks of proceeds from foreign illicit activities flowing through or into our system, as a transit or integration/destination point.
  - Such flows could be through the use of shell/front companies, and/or professional intermediaries.
- **Amount of assets and funds**, flowing through and being managed in Singapore has **grown over the years**, in tandem with the economic growth and development of Singapore and the region.



Increased complexity of ML/TF/PF risks

- **Risks becoming more complex**, due to the geo-political climate, macro-economic global events, and the increased use of sophisticated structures.
  - Singapore is also exposed to **regional risks and threats** (e.g. corruption, tax evasion, cyber-enabled fraud, etc.)
- Technological advancements have also provided **increased opportunities and channels for criminals to launder or move their illicit funds and assets across jurisdictions, with speed and ease.**
  - Singapore's status as a Fintech hub has made us an attractive place of business for virtual assets – **virtual assets** (digital payment tokens) and digital payments sectors keen to gain foothold here.



# Overview of Singapore's Dynamic Risk Monitoring Approach

*Fast changing and increasingly complex risks necessitate agility and dynamism*



Since the last FATF Mutual Evaluation, **Singapore has adopted a dynamic approach** to risk monitoring and assessments to keep pace with the changing risk landscape and typologies.



Risk surveillance and monitoring performed through:

- **Risks and Typologies Inter-Agency Group**, which allows agencies to share on ongoing basis, information on surveillance outputs (e.g. networks of concern) and significant cases for collective action,
- **Working with industry** (e.g. through engagements by agencies, publication of best practices and guidance papers) to raise collective risk awareness, and
- **Published risk assessments on specific risk themes**, such as TF, Legal Persons, Legal Arrangements, Virtual Assets and Environmental Crimes ML.

**National Risk Assessments** are published to synthesise Singapore's understanding of key ML/TF/PF threats and risks, taking into account observations and risk assessments by agencies as well as feedback from the private sector and foreign authorities over the years.





# Publication of Singapore's Risk Assessments and National Strategies

Money Laundering  
National Risk  
Assessment

National Anti-  
Money Laundering  
Strategy

Proliferation  
Financing National  
Risk Assessment &  
CPF Strategy

Virtual Assets Risk  
Assessment

Terrorism  
Financing National  
Risk Assessment

Strategy for  
Countering the  
Financing of  
Terrorism

Environmental  
Crimes Money  
Laundering  
National Risk  
Assessment

Legal  
Arrangements Risk  
Assessment

Law Enforcement  
Strategy to  
Combat ML

Legal Persons  
Risk Assessment



Refer to [ACD Website](#) for more  
details – Notices  
from the Registrar



# **ML NRA and National AML Strategy**



# Singapore's Key ML Threats

## Key ML Threats



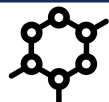
### **Fraud**, particularly cyber-enabled fraud

- High number of cases from foreign fraud
- Marked increase in threat from cyber-enabled fraud targeting Singapore residents by overseas syndicates
- Threat exacerbated by advancements in digitalisation - key crime of concern globally
- Key threat highlighted by other jurisdictions through engagements with foreign authorities



### **Organised Crime**, especially illegal online gambling associated with foreign-organised criminal groups

- Layering of illicit funds through multiple jurisdictions
- Assets seized/prohibited from disposal in recent major ML case are suspected to be proceeds from illegal online gambling



### **Corruption**, originating from abroad

- Layering of illicit funds through multiple jurisdictions
- Assets seized/prohibited from disposal in recent major ML case are suspected to be proceeds from illegal online gambling



### **Tax Crimes**, originating from abroad

- Inherent threat as wealth management hub
- Increase in number of incoming foreign requests, related to tax offences
- Legal persons/arrangements and complex structures used to hold and move funds and assets



### **Trade-Based Money Laundering**









- Inherent threat as trading and transportation hub
- Increase in requests from foreign counterparts
- Involve techniques such as over/under invoicing of goods, and use of financial and professional intermediaries



# Higher ML Risk Sectors

Similar to many other international financial centres, banks pose the highest ML risks to Singapore

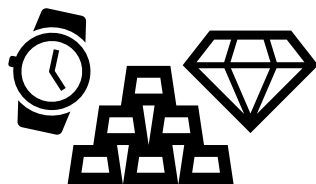
*There are also other higher ML risk sectors which are susceptible, in spite of controls in place, due to (i) abuse by virtue of their roles as professional / financial intermediaries, (ii) exposure to cross-border transactions, and/or (iii) placement in high value assets*

<div><b><u>Corporate Service Providers</u></b><ul style="list-style-type: none"><li>• Linked to misuse of legal persons in some instances - legal persons are featured in ML cases, including fraud, corruption/tax and trade-based money laundering</li></ul></div>	<div><b><u>Digital Payment Token Services Providers</u></b><ul style="list-style-type: none"><li>• Increased in reported cases related to Digital Payment Tokens (DPTs)</li><li>• International typologies noted ways in which DPTs can be exploited for cross border transactions</li></ul></div>	
<div><b><u>Real Estate</u></b><ul style="list-style-type: none"><li>• High value, good store of value and provides opportunity to launder funds</li><li>• Typologies related to fraud, corruption/tax ML risks</li></ul></div>	<div><b><u>Casinos</u></b><ul style="list-style-type: none"><li>• Cash intensive, exposure to foreign customers, source of wealth or funds from overseas</li><li>• Typologies indicate inherent ML threats</li></ul></div>	<div><b><u>Precious Stones and Precious Metal Dealers</u></b><ul style="list-style-type: none"><li>• Good store of value, cash focused</li><li>• Typologies indicate inherent threats</li></ul></div>
<div><b><u>Payment Institutions Offering Cross Border Money Transfers</u></b><ul style="list-style-type: none"><li>• Cross-border activities; exposure to higher risk customers</li><li>• Typologies indicate misuse, including by shell companies, for movement of funds across borders</li></ul></div>	<div><b><u>Licensed Trust Companies</u></b><ul style="list-style-type: none"><li>• Exposed to higher risk customers, including those with corruption/tax evasion ML risks</li><li>• Deal with complex structures (featuring legal arrangements), high value, and cross-border transactions</li></ul></div>	<div><b><u>External Asset Managers</u></b><ul style="list-style-type: none"><li>• Exposed to higher risk customers including those with corruption/tax evasion ML risks</li><li>• Deal with complex structures, high value, and cross-border transactions</li></ul></div>



# National AML Strategy

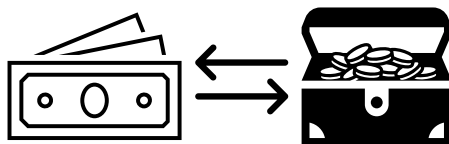
## Sector Risk



**PSMDs:  
Medium-High**



**Moneylenders:  
Medium-Low**



**Pawnbrokers: Low**

## AML Strategy

**Prevent**

**Detect**

**Enforce**

Whole-of-  
Society  
Coordination  
and  
Collaboration

Legal and  
Regulatory  
Framework

International  
Cooperation





# PF NRA and CPF Strategy



# Singapore's Key PF Threats

From **PF-related intelligence** that Singapore has received from our international partners, most commonly featured threats are:

- **Ship-to-ship transfers** (around 45% of intelligence received)
- **Movement of dual-use goods** (around 20%)
- **Export of luxury goods** (around 20%)

From **PF investigations** initiated by Singapore authorities, most commonly featured threats are:

- **Ship-to-ship transfers** (around 42%)
- **Export of luxury goods** (around 25%)
- **Misuse of legal persons** (around 17%)
- **Misuse of virtual assets** (around 17%)



# Higher-PF Risk Sectors

- **Banks are exposed to higher PF risks** in light of the wide range of services they provide and large volume of legitimate transactions that they process on a daily basis, as well as international typologies and the cases that have been observed in Singapore.
- **Digital payment token service providers are exposed to some PF risks** given international typologies and their activities which entail dealing with virtual assets that are known to be misused by individuals and entities involved in the proliferation of WMD and PF.
- Among the DNFBP sectors, **corporate service providers are exposed to some PF risks** given international typologies and their role in the formation of companies, and some corporate service providers may be the directors of these companies.

Sectors assessed	
Financial sectors	
Banks	Higher PF risks
Digital payment token service providers	Some PF risks
Remittance agents (i.e. cross-border money transfer service providers)	Sector to watch
Maritime insurers	Sector to watch
DNFBP sectors	
Corporate service providers	Some PF risks
Precious stones and precious metals dealers	Sector to watch
Lawyers	Sector to watch



# CPF Strategy

## Approach to Combat PF



Maintaining strong domestic and international cooperation



Being alert to evolving PF risks



Keeping regulations updated



Industry engagement



Monitoring compliance, and taking proportionate and effective enforcement actions



# Virtual Assets Risk Assessment (VARA)



# VARA

Virtual assets sector is **rapidly evolving**

PSMDs could be **exposed to ML/TF/PF risks when accepting digital payment tokens** e.g. cryptocurrencies



Singapore maintains close oversight of the emerging risks to ensure its AML/CFT/CPF frameworks remain effective

To manage the risks, strict compliance requirements are imposed on licensed entities

Singapore also collaborates internationally and conduct regular surveillance and supervision



# TF NRA and Strategy for CFT





One Home Team - Together, We Keep Our Home Safe & Secure

# Singapore's TF NRA



# Terrorism (Suppression of Financing) Act 2002

- An Act to suppress the financing of terrorism
- Prohibits:
  - Providing or collecting property for terrorist acts
  - Providing property and services for terrorist purposes
  - Using or possessing of property for terrorist purposes
  - Dealing with property of terrorists
- Penalties:
  - For Individuals:
    - A fine not exceeding S\$500,000, 10 year imprisonment, or both.
  - For Companies:
    - A fine not exceeding S\$1 million, or twice the value of the property or service provided, **whichever is higher.**

# Terrorism (Suppression of Financing) Act 2002

- Duty to disclose to the Police so long as:
  - A. You have in your possession or control any property belonging to any terrorist or terrorist organisation; or
  - B. Information about any transaction or proposed transaction
- Penalties for failure to disclose:
  - For individuals who encounter the property or information in the course of their work:
    - A fine not exceeding S\$250,000 or a maximum jail term of 5 years, or both
  - For companies:
    - If it is (A), **the higher of** S\$1 million or twice the value of the property
    - If it is (B), S\$1 million

# Singapore's TF Risks and Context

## Singapore's Geographical Location

- International Financial Centre and transport/transshipment hub in Southeast Asia

## Regional Terrorism/TF Threats

- Active terrorist groups in Southeast Asia
  - ISIS, Al Qaeda, JI
- Potential spillovers from Middle East conflicts

## (New) Developments Since 2020

- Rapid growth of digital economy
  - Cross-border fast payment systems
  - Digital payment tokens / virtual assets
- **Growth of online fundraising**

## Terror groups in South-east Asia



Sectors at Risk of Being Exploited for TF	2020 TF NRA	2024 TF NRA
Money remittances, including: <ul style="list-style-type: none"> <li>Unlicensed money remittances</li> <li>Cross-border online payments <b>(emerging area since 2020)</b></li> </ul>	High	High
Banks, including: <ul style="list-style-type: none"> <li>New cross-border fast payment systems <b>(emerging area since 2020)</b></li> </ul>	Medium-High	Medium-High
DPT service providers <b>(increased risk since 2020)</b>	Medium-Low	Medium-High
Non-profit organisations, including: <ul style="list-style-type: none"> <li>Online fundraising <b>(emerging area since 2020)</b></li> </ul>	Medium-Low	Medium-Low
Cross-border cash movement	Medium-Low	Medium-Low
Precious stones and precious metals dealers	Medium-Low	Medium-Low
Other AML/CFT regulated sectors not featured in the report (e.g. real estate)	Low	Low
<b>Overall National TF Risk</b>	Medium-Low	Medium-Low

# Traits of Vulnerable PSMDs:

**Varied levels of awareness of TF risks and AML/CFT controls**

**Difficulty in tracing specific items**

- Global market for PS/PM/PP items
- ISIL and Al-Qaeda known to extract PS/PMs for TF

**Rise of Asset-Backed Tokens**

- PS/PM/PPs can be used to back asset-backed virtual assets

# Potential Red Flag Indicators

## **When you are selling:**

- Established customers, including fellow PSMDs, suddenly increasing their purchases of PS/PMs
- Foreign nationals purchasing PS/PMs through multiple transactions over a short time period
- Inconsistency between a customer's profile and the amount of PS/PMs purchased
- Somebody requesting to ship gold to high TF risk jurisdiction

## **When you are buying:**

- Misclassification of gold purity, weight, origin and value on customs declaration forms
- Gold is shipped/transhipped from a high TF risk jurisdiction

Sectors at Risk of Being Exploited for TF	2020 TF NRA	2024 TF NRA
Money remittances, including: <ul style="list-style-type: none"> <li>- Unlicensed money remittances</li> <li>- Cross-border online payments <b>(emerging area since 2020)</b></li> </ul>	High	High
Banks, including: <ul style="list-style-type: none"> <li>- New cross-border fast payment systems <b>(emerging area since 2020)</b></li> </ul>	Medium-High	Medium-High
DPT service providers <b>(increased risk since 2020)</b>	Medium-Low	Medium-High
Non-profit organisations, including: <ul style="list-style-type: none"> <li>- Online fundraising <b>(emerging area since 2020)</b></li> </ul>	Medium-Low	Medium-Low
Cross-border cash movement	Medium-Low	Medium-Low
Precious stones and precious metals dealers	Medium-Low	Medium-Low
Other AML/CFT regulated sectors not featured in the report (e.g. real estate)	Low	Low
<b>Overall National TF Risk</b>	Medium-Low	Medium-Low

## Potential Red Flag and Case Study: Selling of Personal Items by Lone Wolf for TF

In 2019, a terrorist attack took place in Country L and resulted in the death of law enforcement officers, army personnel and the injury of several civilians. The terrorist, known to be affiliated with ISIL, opened fire on army personnel, and detonated an explosive vest after a pursuit and confrontation with law enforcement officers. **Authorities' investigations revealed that the terrorist sold his house furniture and used the proceeds to self-finance his attack.** Proceeds in cash for approximately USD 1000 were used to buy ammunition.



**2024 TF NRA**



**2024 NSCFT**



**Provide Feedback!**





One Home Team - Together, We Keep Our Home Safe & Secure

# Targeted Financial Sanctions Pursuant to TF

# Targeted Financial Sanctions (TFS)

- Singapore is bound by international obligations (UNSC Security Council Resolutions 1267 and 1373; FATF standards) to have a framework for the effective implementation of TFS.
- TFS involves **asset freezing** and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
- All DNFBPs, including PSMDs, pawnbrokers and moneylenders, play an important role as gatekeepers.

# Terrorism (Suppression of Financing) Act ("TSOFA")

- As part of our efforts to counter terrorism and its financing, an Inter-Ministry Committee on Terrorist Designation ("**IMC-TD**") acts as Singapore's authority for the designation of terrorists.
- **Designation prohibits any person or entity from dealing with or providing any financial assistance to designated terrorists.**
- TSOFA prohibits any person or entity from dealing with any property owned or controlled by, or providing property or financial or other related services while knowing or having reasonable grounds to believe that they will be used by or may benefit, any terrorist or terrorist entity.

## Key Information to Note

- Dealings (whether direct or indirect) with any property owned or controlled by any terrorist or terrorist entity, or which an individual has reasonable grounds to believe will be used to commit any terrorist act are prohibited **with immediate effect** upon designation. The list of persons or entities who have been designated can be accessed via:

### For domestic designations:

Singapore Statutes Online



### For designations maintained by the UN Security Council Committee:

United Nations Security Council



## Key Information to Note

- Screening processes (including ongoing batch screenings conducted between periodic Know Your Client (“**KYC**”) reviews) to detect such persons or entities (and their relevant parties) should be in place, including due diligence checks before entering into any business relationship or transaction with such persons or entities, and on an ongoing basis (particularly when there is a new designation).
- Any information about transactions or proposed transactions related to any property, funds, or other assets belonging to any terrorist or terrorist entity (including information that could prevent a terrorism financing offence or assist in apprehending, prosecuting or convicting someone for such an offence) should be disclosed to the Police **immediately**. No criminal or civil proceedings will be taken against a person for any disclosure made in good faith.

## Key Information to Note

- Any funds or assets related to these persons or entities should be frozen **immediately** (within 24 hours of designation) and **without prior notice**. Further, you should not enter into transactions or provide services to these persons and entities, and should file an STR.
- You should not inform individuals of assets frozen / STRs filed against them, or any other information or matter which will likely prejudice any proposed or ongoing investigation by the Police.
- You will be subject to periodic/risk-triggered inspections/interventions by MinLaw on your CFT controls and implementation of TFS measures.

# Penalties for Breaches of TFS Obligations

- **Stringent criminal penalties** in place for breaches of TFS obligations, including breaches in the prohibition against dealing in the funds/assets of designated individuals (s.6 of TSOFA) or failure to disclose information about any transaction or proposed transaction in respect of terrorist property (s.8 of TSOFA).
- Penalties include up to 10 years imprisonment and a fine not exceeding \$500,000 or both (for offences under s.6); or up to 5 years imprisonment and a fine not exceeding \$250,000 (for offences under s.8).
- In addition, an entity may be subjected to **regulatory penalties** (including fines of up to \$100,000 etc.) for failing to take the necessary measures to implement TFS.



# Maintaining Robust CFT Controls

## Subscribe

Stay up-to-date by subscribing to UNSC and MAS webpages for latest information on targeted financial sanctions.

## Screen

Ensure due diligence checks and timely freezing against list of designated subjects and persons whom your business/sector may have been notified by the authorities from time to time.

## Report

Promptly file suspicious transactions reports.

## Comply

Ensure compliance with TSOFA by having internal frameworks and processes in place.

# Subscribe to MAS and UNSC Consolidated Mailing Lists

Scan code to subscribe to MAS Mailing List for updates to the lists of designated individuals and entities



Scan code to subscribe to UNSC Consolidated Mailing List for updates to the list of internationally-designated persons and entities by UNSC



# Screen

**Screening** processes should be in place to detect such persons and entities, who should not be dealt with, and any funds or assets related to these persons or entities should be frozen **immediately**.

- Ensure screening databases are updated.
- Entities should also be alert to individuals/entities assisting in the evasion of sanctions including persons who may not be designated, such as family members, close associates of designated individuals.
- Keep records of due diligence checks.

**The FATF requires the freezing of funds/assets and imposition of financial restrictions on not only designated entities/individuals but also entities/individuals/persons acting on their behalf or at their direction.**

**Similarly, Section 6(1)(c) of TSOFA makes it an offence to provide any financial services (or any other related services) in respect of any property that an individual knows (or has reasonable grounds to believe) is owned or controlled by any terrorist or terrorist entity, or for the benefit of, or on the direction or order of, any terrorist or terrorist entity. This includes funds derived or generated from property owned or controlled, directly or indirectly, by any terrorist or terrorist entity.**

# Report

- Maintain vigilance against TF-related red flags and promptly **file STRs**.
  - Reporting entities may refer to a bulletin titled – ‘Red Flag Indicators for Terrorism Financing’ published on Suspicious Transaction Reporting Office (“**STRO**”)’s SONAR platform on 27 December 2023 for a list of TF-related red flag indicators for reference.
  - When filing STRs on TF matters, reporting entities should indicate the reference code (CFT Oct 2023) in the ‘Notice Reference Number’ field under the ‘Reporting Institution’ tab.
- To consider leveraging data analytics as part of the processes for TF risk detection and monitoring.

There is **no need** to identify an underlying offence, for an STR to be filed. An STR should be filed as long as your entity has a reasonable suspicion that any transaction or **potential/proposed** transaction could involve the funds and assets of designated persons or entities.

# Red Flag Indicators for TF

- Entities must familiarise themselves with the STRO's sector-specific **red flag indicators** of a suspicious transaction and **file an STR** if any red flag indicators are met.
- Examples of red flag indicators include but are not limited to:
  - Anomalies noted during customer/supplier due diligence
  - Unusual fund movement
  - Structuring/layering of transactions
  - Transactions with no apparent business/lawful purpose
  - Unusual transactions with higher TF risk jurisdictions

**Sector-specific red flag indicators can be downloaded from Suspicious Transaction Reporting Office (STRO)**

Scan code for  
**List of jurisdictions\* subject  
to call for action and/or  
under increased monitoring  
by FATF**



# Comply

- Review existing screening frameworks and processes to **ensure compliance** with TSOFA.
- Familiarise yourself with your regulators' supervisory expectations & requirements with regards to AML/CFT controls. This generally includes:
  - Having internal policies, procedures and controls in place to comply with AML/CFT/CPF obligations including conducting KYC and CDD/ECDD checks;
  - Requirements to identify, assess and understand the risks of TF;
  - Adhering to record-keeping requirements; and
  - **Specific to TFS**, taking reasonable measures to assess whether a client/customer or any person on whose behalf a customer is acting for, and any beneficial owner of that person, is a designated individual. If so, your business must decline to enter into any transaction or terminate any existing transactions with the customer; and file an STR.

## Other Useful Resources

MAS' Information Paper on Strengthening  
AML/CFT Name Screening Practices



Guidance on PF in the Guidelines to MAS'  
AML/CFT Notices PSN01 and PSN02



MAS' Guidance on Sound Practices to Counter  
Proliferation Financing



You may also wish to refer to the FATF website  
for more information  
e.g. FATF Glossary





---

One Home Team - Together, We Keep Our Home Safe & Secure

# Thank you



# Additional Guidance

- **Assessment of Customer Risk**
- **Identification of Material Red Flags**
- **SOW Corroboration**
- **Ongoing Monitoring of Customers and Transactions**
- **STR Filing Timelines**



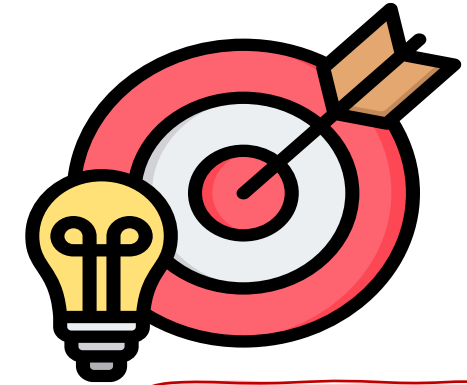
# IMC Report Oct 2024

## Purpose of IMC Review

- Prompted by lessons from a significant ML case in 2023
- To review Singapore's AML regime and ensure that it stays up to date with increasing sophisticated crimes
- Participated by multiple government agencies and covered FIs and gatekeepers, such as PSMDs

## Recommendations Relevant to Your Sectors

- Strengthen AML standards for gatekeepers
- Sector supervisors to further support gatekeepers in enhancing their capabilities to combat ML
- Deepen channels for data sharing amongst and with gatekeepers



Refer to Press  
Release on [MOF  
Website](https://www.mof.gov.sg/press-releases) for more  
details



# The 3 Stages of ML

## Placement

Criminal places his dirty money in legitimate financial system, by:

- Incorporating a shell company through a corporate service provider
- Creating a corporate bank account for the shell company at a bank
- Engaging a lawyer, to receive monies in his client account, which is later transferred to shell company's bank account

## Layering

Criminal conceals the source of his wealth, by:

- Obtaining a mortgage from the bank
- Purchasing a property through a real estate salesperson
- Engaging a lawyer for conveyancing services
- Obtaining tax advice from an accountant

## Integration

Criminal completes laundering his money, by:

- Engaging a real estate salesperson to sell the property, receiving his now-clean money and a profit from the sale
- Using laundered money to purchase high value items, including jewellery and luxury watches from PSMDs



# Assess Customer Risk and Identify Material Red Flags

## Understand Customer Profile

- Understand customer's profile to properly conduct a ML/TF/PF risk assessment of customer/ transaction and ongoing monitoring of business relationships
- Document customer profile and customer risk assessment conducted

## Exercise Vigilance

- Exercise vigilance in identifying ML/TF/PF red flags during CDD process
- Pay attention to discrepancies between customer's representation and documents provided, or information from other sources
- Always conduct further follow-up actions when in doubt

## Set Guidance to Identify and Escalate Red Flags

- Communicate staff's roles and responsibilities
- Set clear guidance for staff to take reasonable steps to identify and escalate material red flags, such as the type of material red flags to look out for, what follow-up action to take when red flags are encountered and when to escalate to compliance function and senior management

## Conduct ECDD for High Risk Customer/ Transaction

- Where material red flags are detected, customer/ transaction should be assessed as having high ML/TF/PF risk and ECDD should be conducted
- Document ECDD conducted, e.g. SOW corroboration, Senior Management approval



# Examples of Material ML/TF/PF Red Flags

- Transactions which are inconsistent with customer's known profile
- Significant discrepancies between customer's representation against information/document from independent sources
- Payment received from unrelated third parties
- Unusual payment arrangements
- Unusually large transactions (cash or non-cash)
- Unusually complex transactions
- Transactions with no apparent or visible economic or lawful purpose



Scan to download  
[Guidelines for  
Regulated Dealers](#)  
(refer to Annex D  
for list of red flags)

**Regulated entities should conduct ongoing monitoring of customer transactions against the known customer profiles to detect inconsistencies**



# Examples of Material ML/TF/PF Red Flags



[Pawnbrokers](#)



[Moneylenders](#)



# Supervisory Observations

## Good Practices Observed

- **Material red flags identified and followed up by dealers—**
  - A customer who returned on the same day to purchase more gold bars in cash, which was not usual in that instance
  - A purchase of gold bars using Bitcoin with intention of selling back the gold bars immediately for a payout to a bank account
  - A purchase and sell back of gold bars within a short period of time, incurring losses

## Areas of Weaknesses Observed

- Customers/transactions were assessed to be low ML/TF/PF risks **solely** based on negative screening results or payments were received from financial institutions even when material red flags were present
- **Material red flags not identified and followed up by dealers—**
  - A customer made exceedingly high level of purchases over a period of time. The dealer was aware that the customer was a housewife and her SOW was supposedly from her husband but there was no attempt to establish the husband's SOW
  - Payments were received from an unknown third party from overseas via telegraphic transfer
  - Payment were received from overseas bank accounts of foreign companies which the customer claimed that she was a director/owner



# SOW Corroboration



## Why is SOW important?

- Help to determine the legitimacy of the customers' funds
- Needed for proper ongoing monitoring of customers
- Guard against ML/TF/PF and reputational risks of dealing with illicit assets



## What is expected of regulated entities?

- Take appropriate and reasonable measures to establish SOW and independently corroborate customer's representation
- Obtain basic SOW information and corroborate SOW where ML/TF/PF risk is heightened
- Apply rigor in assessing the plausibility of customer's SOW and avoid over-reliance on customers' representation
- Closer senior management oversight and enhanced monitoring where SOW could not be established
- Should not assume funds received through FIs are legitimate
- May consider a range of measures to establish SOW of customers in a risk proportionate and reasonable manner

## Key Principles in Establishing SOW of Customers



### Materiality

Focus on:

- Whole entire body of wealth to the extent practicable and possible
- High risk SOW
- Whether residual risk of uncorroborated wealth is acceptable



### Prudence

- Use more reliable corroborative information
- Ensure assumptions or benchmarks used are reasonable, relevant and appropriate
- Document and periodically review benchmarks and assumption used
- Benchmarks and assumptions should not be used when there are reasons to suspect



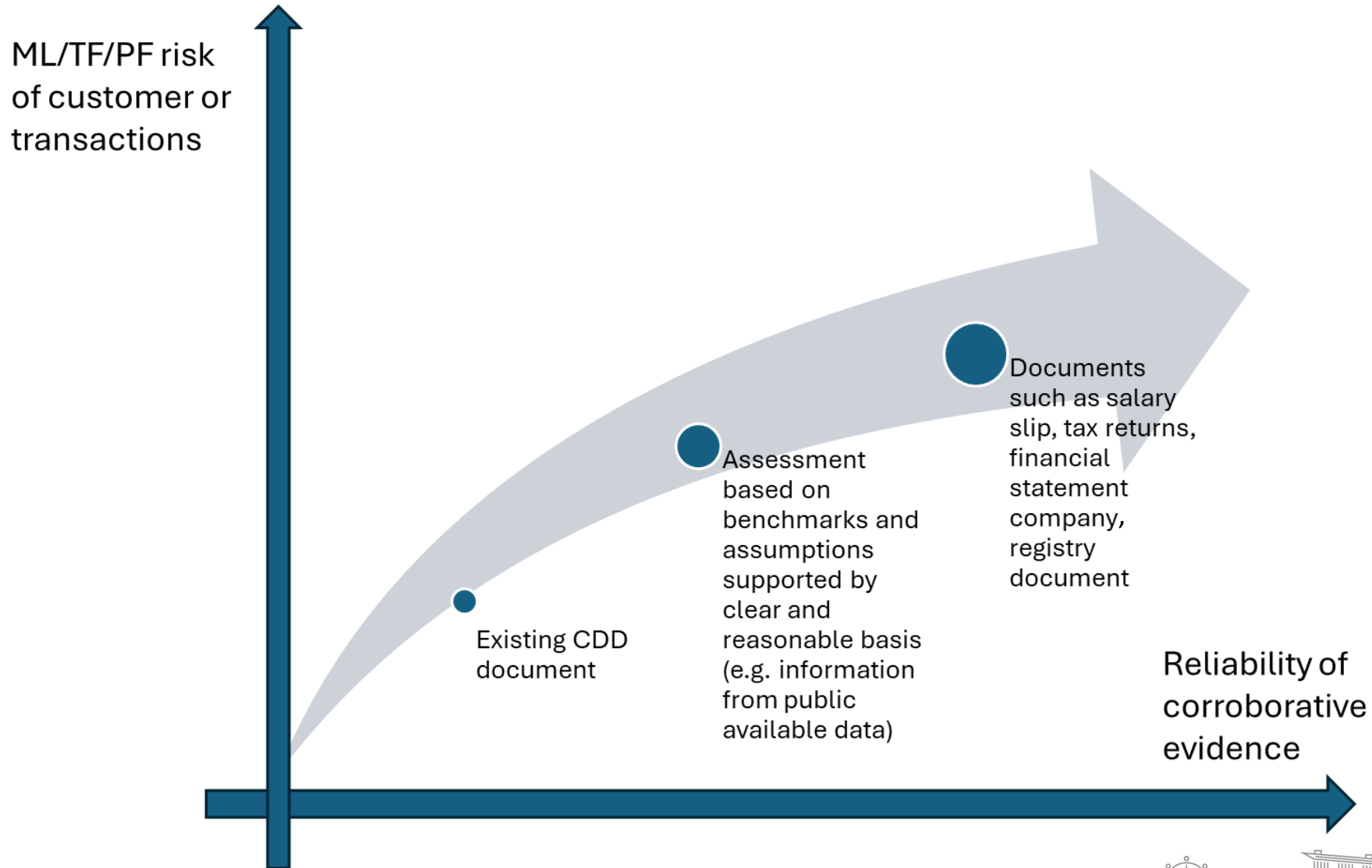
### Relevance

- Obtain pertinent, fit-for-purpose corroborative evidence to extent practicable
- Exercise reasonable judgement when reviewing information and documents
- Utilise independent and reliable documents and information, where possible





# Adopt Risk-Based Approach in Designing SOW Checks



# Supervisory Observations

## Good Practices Observed

- A PSMD noted that the payments for a customer's jewellery were to be received from a third-party company. The PSMD enquired on the relationship between the customer and the company and requested the customer to furnish the company ownership reports to support his claim that he owned the company
- As part of ongoing monitoring, the PSMD detected a high level of bullion accumulated and requested for more information on the customer's SOW and SOF
- A customer attempted to purchase gold bars with S\$10,000 bills and informed that he was in the business in oil, textile and others. The PSMD went on to enquire on where the cash was withdrawn from, in Singapore or overseas, and the details of his business

## Areas of Weaknesses Observed

- For cash transactions between \$330,000 to \$440,000 each, a PSMD accepted the clients' representation that they were businessman/manager and did not make further enquiries or take measures to establish their SOW
- A customer purchased a diamond which was closed to \$1million which was significant and unusually higher than the PSMD's other sales. The PSMD did not take reasonable measures to corroborate the customer's SOW/SOF even though the purchase was not in line with the customer's known profile (Office Operation Director and later property agent)
- A PSMD entered into designated transactions with customer from a country which Registrar notified to have inadequate measures to prevent ML/TF/PF and did not conduct ECDD measures



# Additional Guidance

## PSMDs



Refer to [ACD Website](#)  
for more details –  
Notices from the  
Registrar

## Pawnbrokers



Refer to [Registry of  
Pawnbrokers Website](#)  
for more details –  
AML/CFT/CPF  
Resources

## Moneylenders



Refer to [Registry of  
Moneylenders Website](#)  
for more details –  
AML/CFT/CPF  
Resources



# STR Filing Timelines

## 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

- STRs should be filed as soon as reasonably practicable upon the establishment of suspicion

## What is “as soon as reasonably practicable”

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



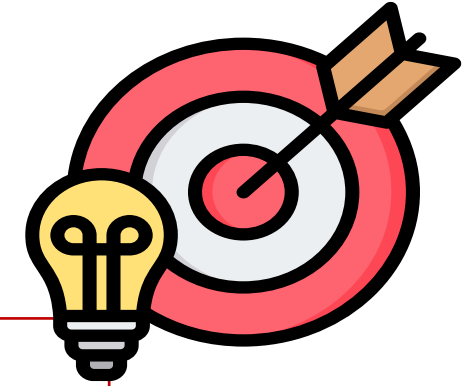
E-file on the Police  
webpage via [STRO  
Online Notices And  
Reporting platform](#)  
(SONAR)



# Enforcement



# Enforcement Principles



## Enforcement Objectives

- Foster high standards of compliance and to deliver **fair and effective** enforcement outcomes to **deter** regulatory infractions and **preserve trust** in the regulated sectors

## Enforcement Principles

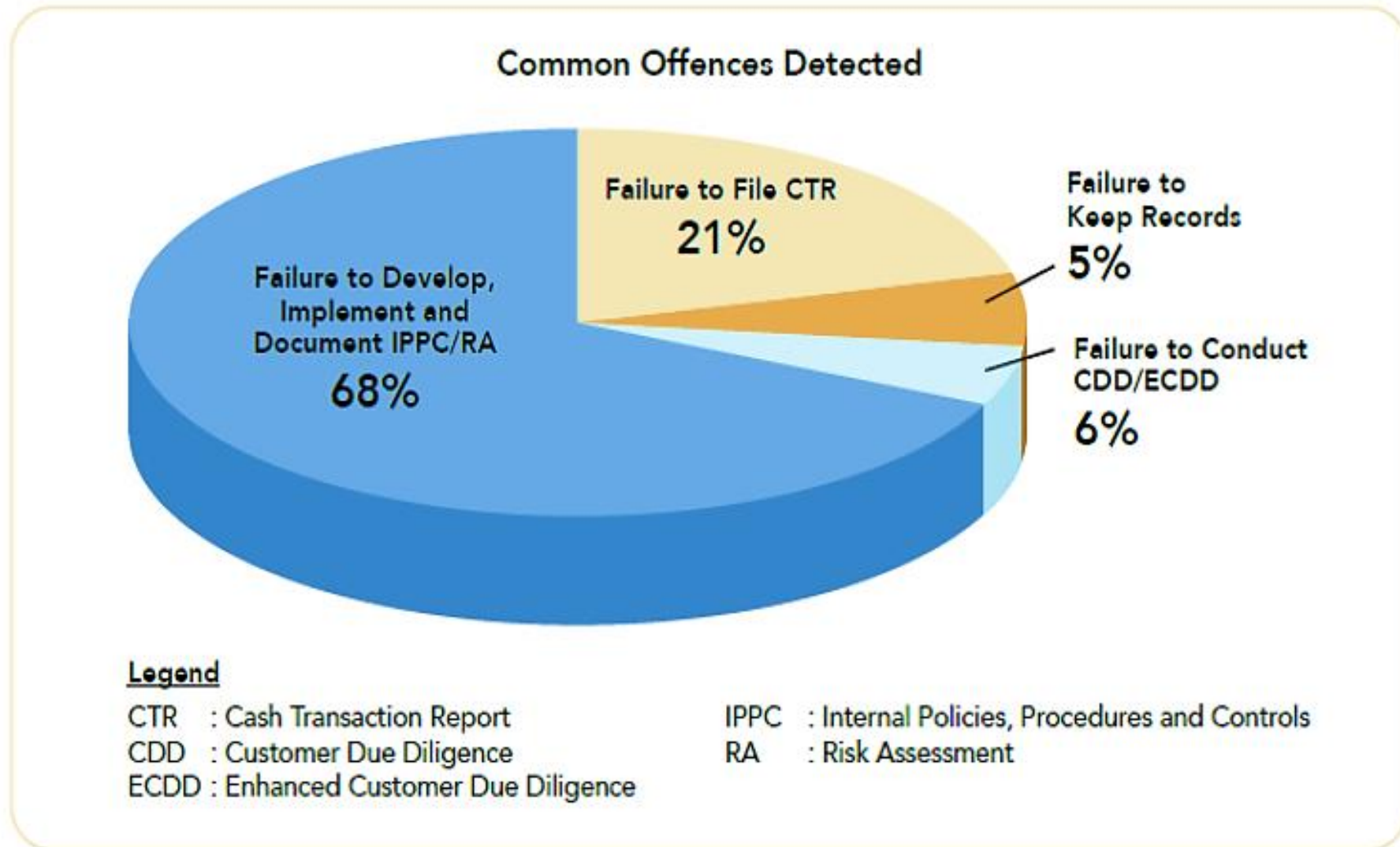
- **Detect** Regulatory Offences and Breaches Early
- **Impose** Effective Sanctions and Deterrence
- **Shape** Desired Regulatory Behaviour



Scan to download  
[2025  
Enforcement  
Report](#)



# Offences (2021 to 2024)



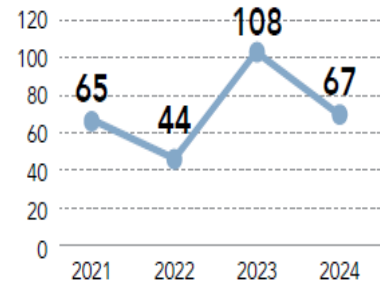
# Inspections, Investigations, Enforcement (2021 to 2024)

**777**  
Inspections

**1,060**  
Investigations

**222**  
Enforcement  
Actions

## Warning

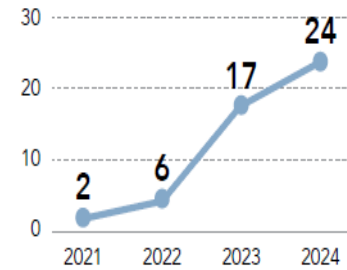


284 Warnings were issued during reporting period

### Top 3 offences

- Unregistered dealings
- Failure to submit IPPC/RA
- Failure to submit SAR

## Composition

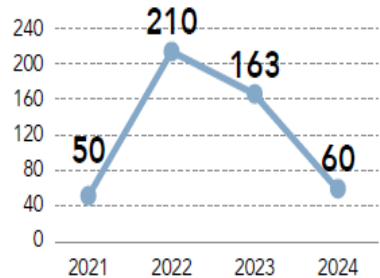


\$639,250 in composition penalties offered during reporting period

### Top 3 offences

- Unregistered dealings
- Failure to file CTR, conduct CDD/ECDD
- Providing false information

## Advisory

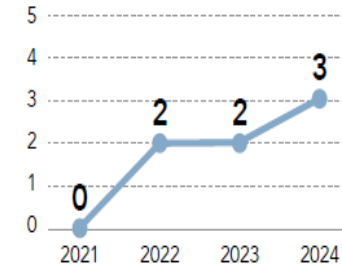


483 Advisories were issued during reporting period

### Top 3 offences

- Failure to notify Registrar of change in place of business/particulars
- Unregistered dealings
- Failure to file CTR, conduct CDD/ECDD

## Cancellation



7 Cancellations of Certificate of Registration for breach of registration conditions



# Enforcement Cases

## Composition Fine for Providing False Information to the Registrar

- In Oct 2022, the Registrar imposed a composition fine on a regulated dealer who provided false information to the Registrar during the renewal of the entity's Certificate of Registration ("COR").

## Composition fine for Unregistered Dealings

- In Oct 2023, the Registrar imposed a composition fine on a registered dealer and its compliance officer for carrying out unregistered regulated dealings when the COR lapsed.

## Enforcement Actions Against Directors and Compliance Officers for Offences by Corporations

- Enforcement actions including imposing composition fines against 5 individuals, and issued warnings and advisories against 4 other individuals, who were either officers of and/or involved in the management of the PSMD for various offences under the PSPM Act and PMLTF Regulations. The actions were taken as these individuals had either:
  1. Consented, connived or conspired with others to effect the commission of the offence; or
  2. Were, in any other way, knowingly concerned in or party to the commission of the offence, whether by act or omission; or
  3. Knew or ought reasonably to have known that the offence by the corporation would be or was being committed and failed to take all reasonable steps to prevent or stop its commission.

The individuals were found liable for the same offences as the PSMDs.



# FAILURE TO FILE SEMI-ANNUAL RETURNS MULTIPLE TIMES



**FINE**



**Dealer failed to  
submit SAR  
multiple times**

## SAR Submission Period

- 1<sup>st</sup> January – 30<sup>th</sup> January
- 1<sup>st</sup> July – 30<sup>th</sup> July



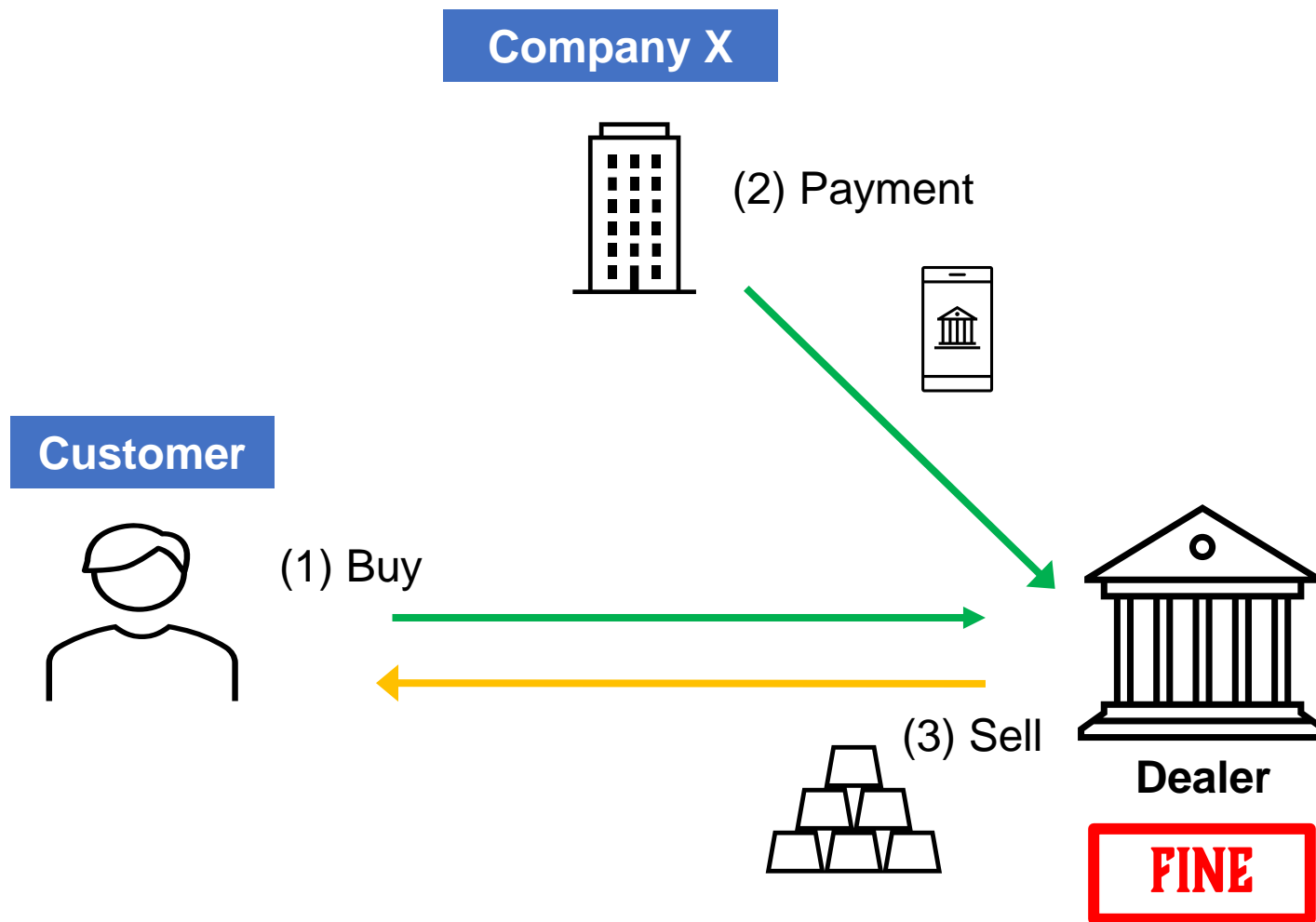
Maximum Penalty for failure to file SAR attracts a fine not exceeding **\$100,000** under Section 18(5) of the PSPM Act.



# Case Studies (Typologies)



# CASE STUDY 1: PAYMENTS RECEIVED FROM UNKNOWN THIRD PARTY



## Transaction Alert

Dear Sir / Madam,

You have received SGD 89,000 on 12 Aug 2022 (SGT) from **ABCDE TRADING PTE. LTD.** to your account via PayNow.

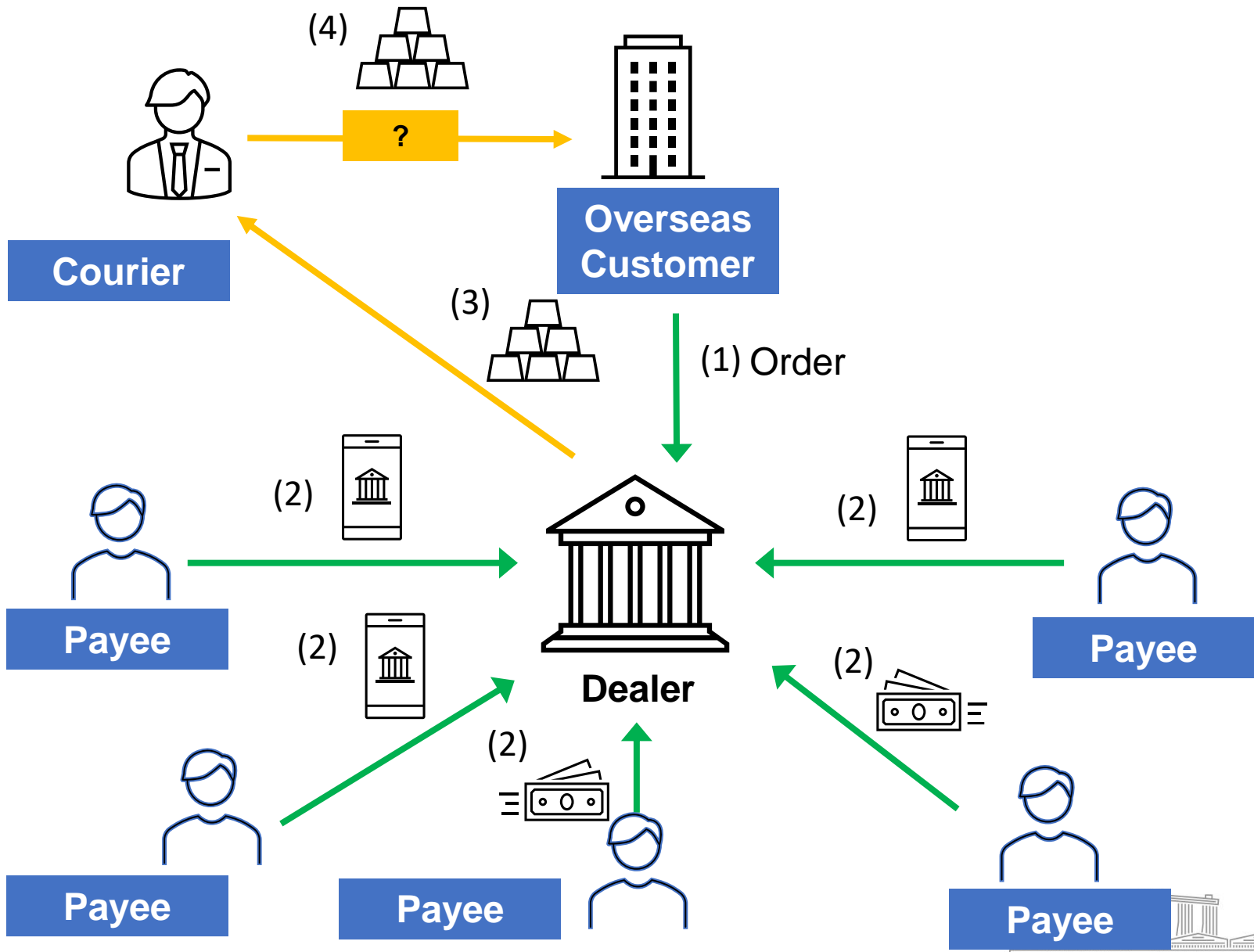
Thank you for banking with us.

Yours faithfully

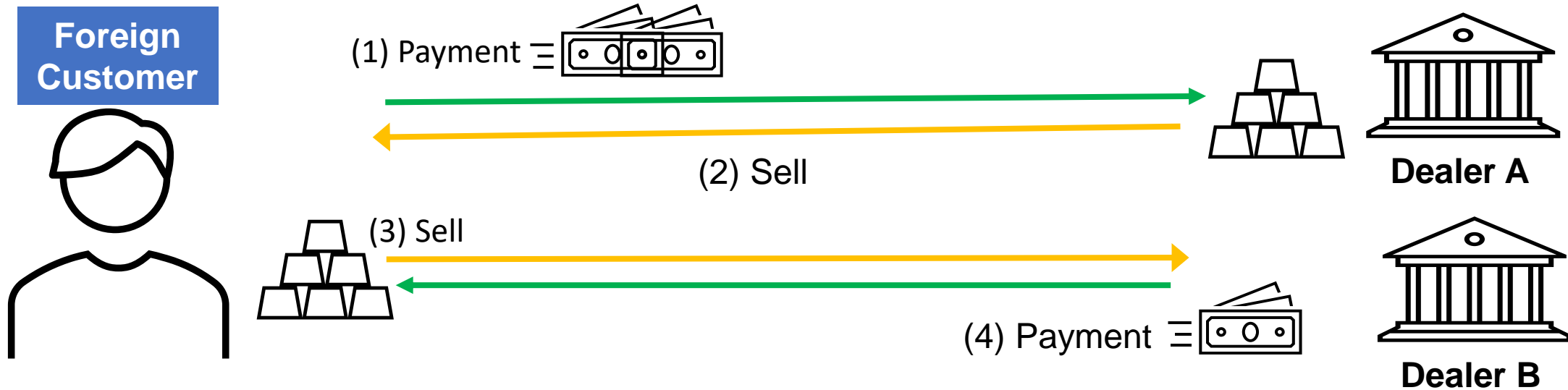
This is an auto-generated message. Please do not reply to this email.



# CASE STUDY 2: PAYMENTS RECEIVED FROM MULTIPLE UNRELATED THIRD PARTIES



# CASE STUDY 3: FOREIGNERS SELLING BACK GOLD WITHIN SHORT TIMEFRAME



## Red Flags

- Foreigners who are in a hurry to sell, and willing to sell at a loss
- Payments made to a corporate bank account or to a different name account

## Where there are reasons to suspect

- Conduct CDD
- Conduct enhanced due diligence such as requesting for purchase documents, reason for selling and/or selling within a short period, reason for transfer to a different name account or receiving large payments in cash
- Consider filing an STR



# Nine Individuals Investigated for Illegal Touting Activities at Changi Airport

- Individuals had approached travellers of the same nationality to solicit them to carry gold and mobile phones back to their home countries.
- These items were intended to be handed over to their counterparts in their home countries, in exchange for a cash reward.
  - Eight individuals had their work passes revoked by MOM and one had his Short-Term Visit Pass cancelled by ICA.
  - All of them were deported and barred from re-entering Singapore.



Scan to access  
Advisory on  
[ACD Website](#)

- Regulated dealers may deal with foreigners on work passes or foreign visitors on short-time visit passes who are acting on behalf of foreign customers.
  - Foreigners on work passes are only allowed to work in the occupation, and for the employer, as approved for their work pass. They are not allowed to operate or participate in any other business.
  - Foreign visitors on Short-Term Visit Passes are prohibited from engaging in any form of business, profession, occupation or employment (paid or unpaid), during their stay in Singapore. The Singapore Government takes a serious view of illegal activities and will not hesitate to take firm action against individuals who flout our laws.

**If you observe any suspicious behaviours or activities that may indicate money laundering or other illegal activities, please lodge a suspicious transaction report. If you witness or suspect a crime in progress, please call 999 for Police assistance.**



# Data Protection – Your Role and Responsibility





# We will cover:

1. Data Breach - Why Should You Be Concerned?
2. Cyber landscape in Singapore
3. Common root causes
4. Understanding your obligations under the PDPA
5. Cyber hygiene



# Why Should You Be Concerned?

## How Data Breaches Impact Company Reputation

### Loss of trust and business

- **65%** of data breach victims lost trust in an organization
- **80%** of consumers will defect from a business if their information is compromised in a breach



### Negative word of mouth

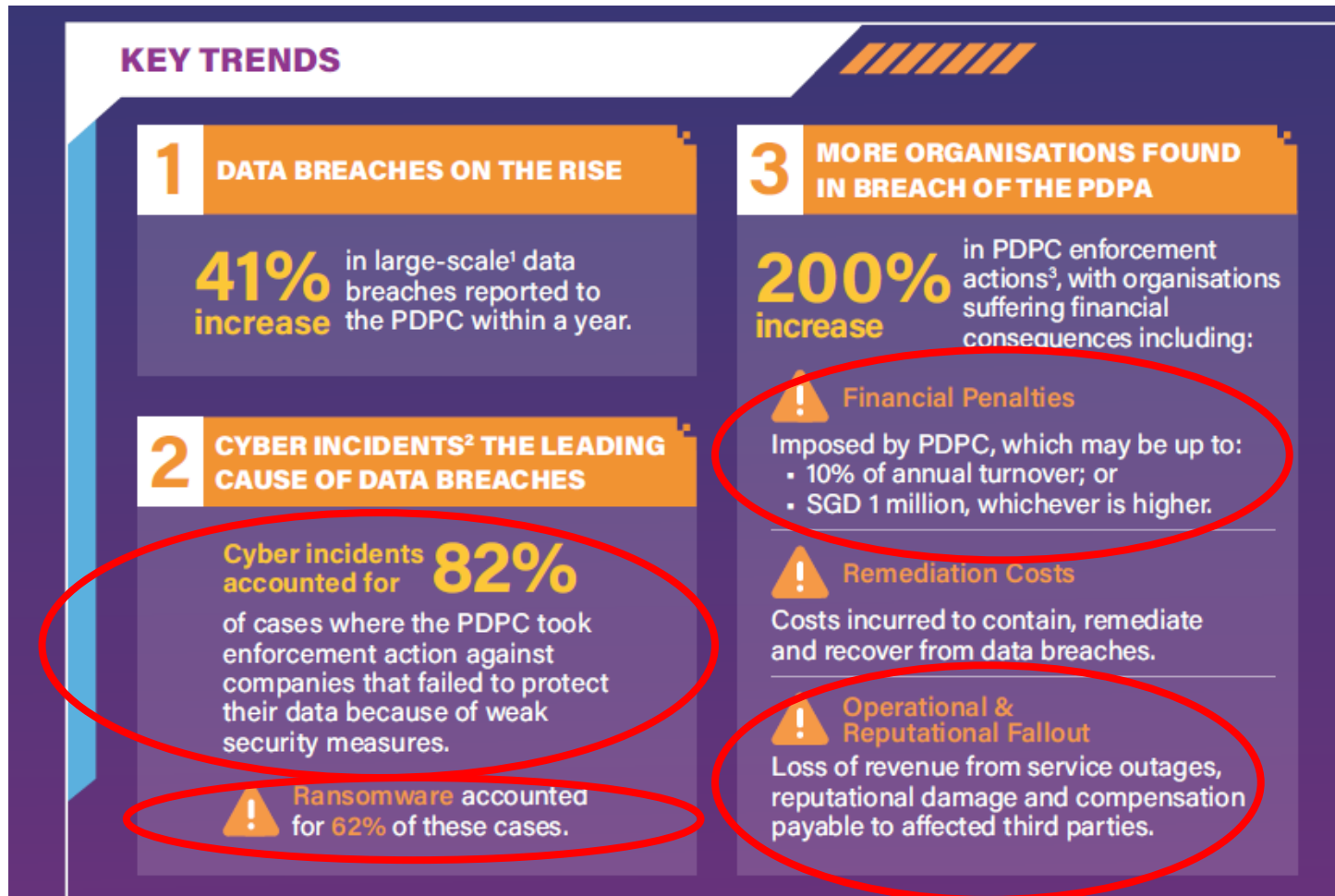
- **85%** tell others about their experience
- **33.5%** use social media to complain about their experience



Source: What's the Damage? The Truth About the Cost of Data Breaches [The Truth About the Cost of Data Breaches](#) | [Terranova Security](#)



# Singapore Data Breach Landscape 2023/2024



Source: <https://www.pdpc.gov.sg/help-and-resources/2025/04/singapore-data-breach-landscape-20232024>



# Singapore Cyber Landscape 2023

## Ransomware Incidents:

**132 cases**

### KEY TRENDS

- The number of ransomware cases in Singapore remained high at 132, same as the number of cases reported in 2022.
- **Top affected industries:** Manufacturing and Construction.

### INSIGHTS & IMPLICATIONS

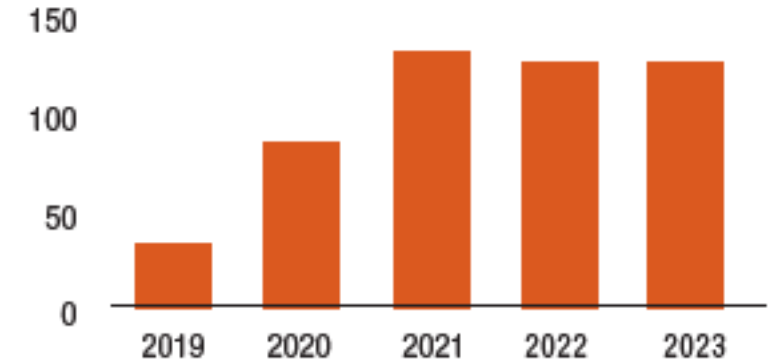
- Globally, the number of ransomware cases hit a record high in 2023, with cybersecurity vendors reporting a 49% increase in victims worldwide as compared to 2022.
- Locally, the construction industry took over the retail industry as one of the top two industries most affected by ransomware. Cybercriminals are highly opportunistic, and will likely pivot to industries that have poor cyber hygiene.

### TIPS TO BE CYBER SAFE

- Organisations can visit the Ransomware Portal launched by the Singapore Police Force, in collaboration with CSA, for ransomware-related resources. These include aid for ransomware victims, advisories, as well as prevention measures that organisations can adopt to avoid falling victim.



Number of ransomware incidents reported to CSA



**If you do not take the necessary prevention measures, then an attack is not a matter of IF, but WHEN!**

Source: Cyber Security Agency of Singapore - singapore-cyber-landscape-2023



# Singapore Cyber Landscape 2023

## Infected Infrastructure:

**70,200 systems**

### KEY TRENDS

- There were around 70,200 infected systems in Singapore in 2023, a 14% decrease from what was observed in 2022. This marked a sustained decline in the number of local infected systems since 2021.

### INSIGHTS & IMPLICATIONS

- While the decline points to an overall improvement in cyber hygiene levels, the absolute number of infected systems in Singapore remains high.
- Based on the dated malware observed in locally-hosted systems, a cause for concern is the **lack of basic cyber hygiene** amongst owners of the infected systems.

### TIPS TO BE CYBER SAFE

- Individuals and organisations should continue to practise good cyber hygiene to prevent their devices from being compromised. For individuals, some tips include: (a) using anti-virus software; (b) being more vigilant in spotting the signs of phishing; and (c) updating software as soon as possible. Organisations can visit the CSA website for cybersecurity toolkits that provide guidance on the adoption of cybersecurity measures for different types of organisations and job roles.



**Are you familiar with cyber hygiene practices?**

Source: Cyber Security Agency of Singapore - singapore-cyber-landscape-2023





# Singapore Cyber Landscape 2023

Are your employees trained to identify phishing attacks?

## Phishing Attempts:

**4,100 cases**

### KEY TRENDS

- Around 4,100 phishing attempts were reported to the Singapore Cyber Emergency Response Team (SingCERT) in 2023, less than half of what was reported in 2022. Notwithstanding the decline, the number of phishing attempts was still about 30% higher than that in 2021.
- **Most spoofed industries:** Banking & Financial Services, Government, and Technology.



### INSIGHTS & IMPLICATIONS

- Globally, phishing cases have continued to rise. **Phishing remains as one of the most popular initial access vectors used by threat actors.** Researchers have also reported on threat actors leveraging AI chatbots to improve the quality of their phishing emails. This means that being able to spot bad grammar or typo errors – which are traditional tell-tale signs of phishing – may no longer be sufficient.

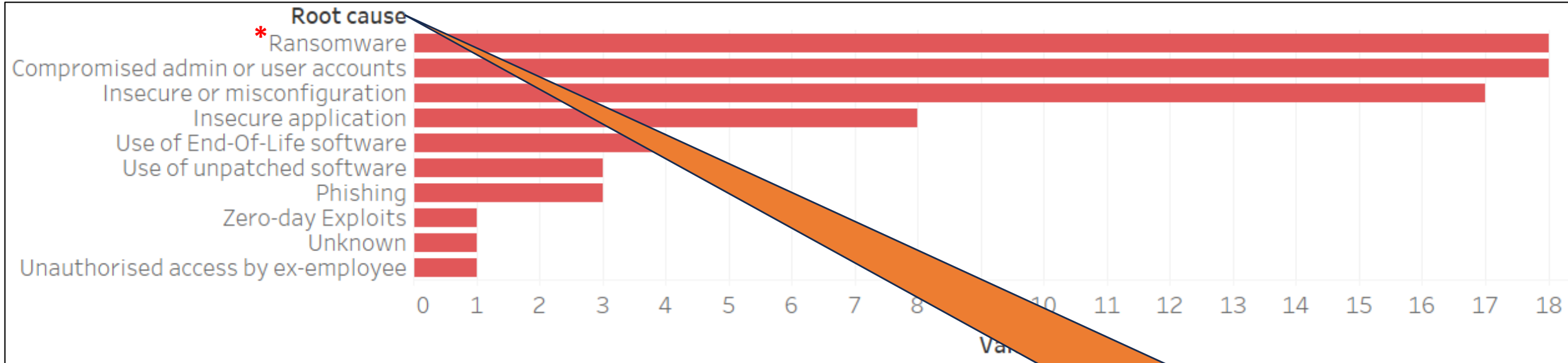
### TIPS TO BE CYBER SAFE

- While AI may have enabled threat actors to improve their use of English in phishing emails, there are other tell-tale signs to look out for. Avoid falling prey by watching out for mismatched and misleading information (e.g. senders' email addresses that masquerade as legitimate ones). Be wary of urgent or threatening language in emails, promises of attractive rewards, or suspicious attachments. Do not click on suspicious URL links, and never disclose your personal or banking credentials to anyone.
- If the phishing link has already been clicked, run a full system scan using anti-virus software. Report the phishing attempt to SingCERT, as well as the organisation that was spoofed (if any).

Source: Cyber Security Agency of Singapore - singapore-cyber-landscape-2023



# Root Causes of Data Breach Incidents: May 2024 to May 2025<sup>1</sup>



**\* While ransomware is not the root cause, it is shown here to demonstrate a correlation with respective root causes. In non-ransomware incidents, data was exposed in clear text.**

**In this session, we will share more about cyber hygiene to address these common root causes.**

## Footnotes:

1. Some incidents involve multiple threat types and are thus counted more than once across categories.

Source: <https://www.pdpc.gov.sg/undertakings>



# Obligations Pertaining to Data Protection

Under Singapore's **Personal Data Protection Act (PDPA)**, administered by the **Personal Data Protection Commission (PDPC)**, private sector organizations are required to comply with **11 key obligations** when collecting, using, disclosing, and managing personal data. Specifically, the below which are related to data protection requirement:

## 6. Protection Obligation

Reasonable security arrangements must be in place to protect personal data from unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

**We will focus on the Cyber Hygiene in the subsequent slides.**

## 10. Data Breach Notification Obligation

Organizations must notify the PDPC and affected individuals of data breaches that result in, or are likely to result in, significant harm to individuals, or where the breach involves large volumes of data.

## 11. Accountability Obligation

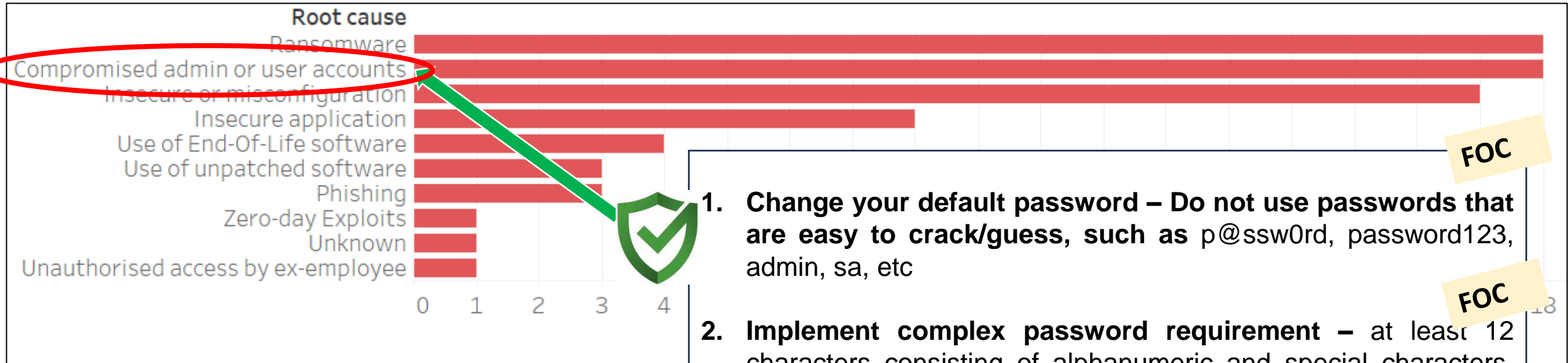
Organizations must designate at least one Data Protection Officer (DPO) to ensure compliance with the PDPA and must make the DPO's business contact information available to the public.

Source: <https://www.pdpc.gov.sg/undertakings>





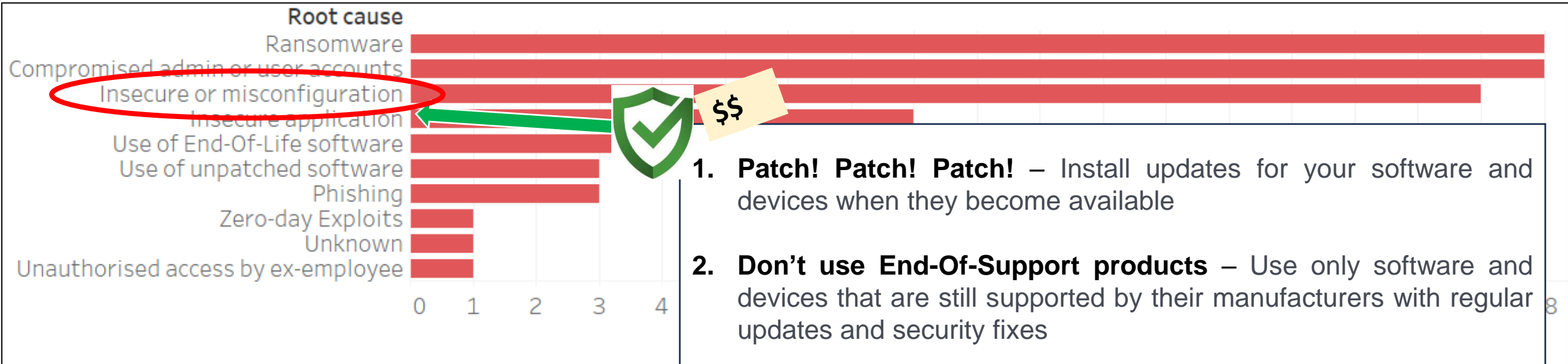
# Cyber Hygiene to Address Common Root Causes



1. **Change your default password – Do not use passwords that are easy to crack/guess, such as p@ssw0rd, password123, admin, sa, etc** FOC
2. **Implement complex password requirement – at least 12 characters consisting of alphanumeric and special characters, e.g. Kopi!Peng#25** FOC
3. **Keep your virus protection up to date** FOC
4. **Implement Multi-Factor Authentication – google authenticator** \$



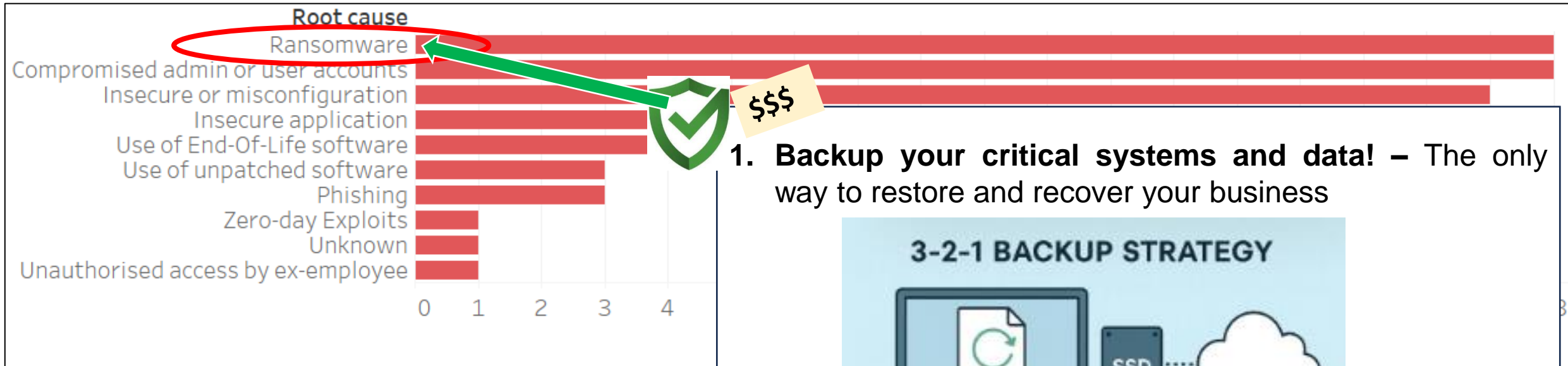
# Cyber Hygiene to Address Common Root Causes



1. **Patch! Patch! Patch!** – Install updates for your software and devices when they become available
2. **Don't use End-Of-Support products** – Use only software and devices that are still supported by their manufacturers with regular updates and security fixes
3. **Scan your systems** - Check your systems regularly for security holes, and test your applications thoroughly to find any weak spots that hackers could exploit
4. Once you find security problems in your systems, make sure to **fix them right away** - don't leave them unpatched



# Cyber Hygiene to Address Common Root Causes



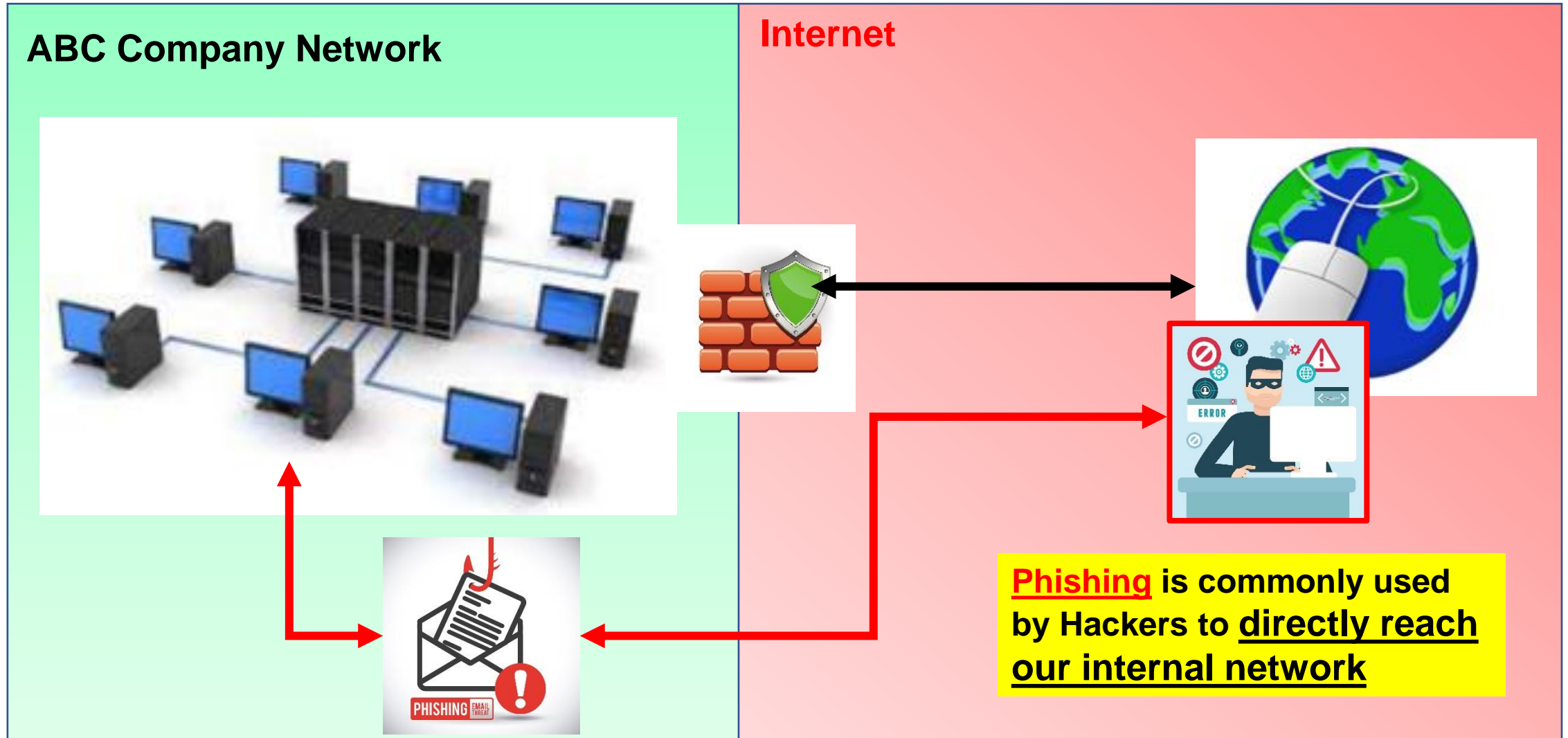
1. **Backup your critical systems and data!** – The only way to restore and recover your business



2. **Encrypt your critical data!** - this way, even if someone steals your data, they can't read or misuse it

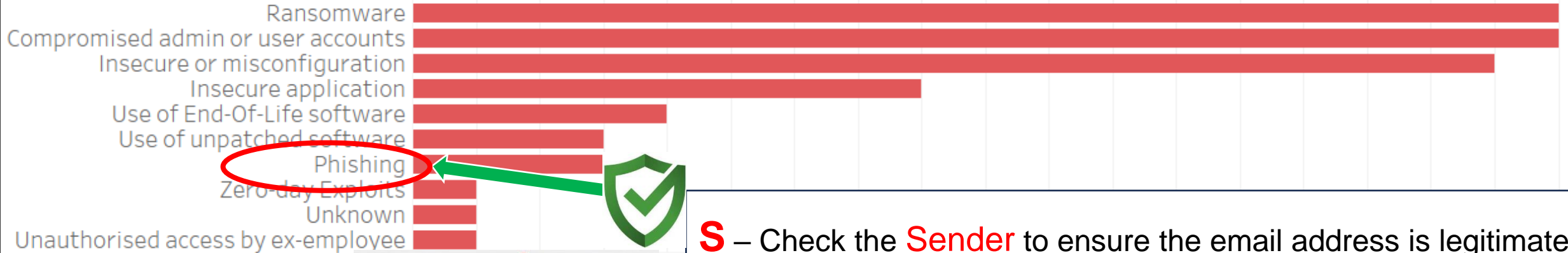


# Cyber Hygiene – Danger of Phishing!



# Cyber Hygiene to Guard Against Phishing

## Root cause



**S** – Check the **Sender** to ensure the email address is legitimate

**L** – Hover over **Links** to verify their destination

**A** – Be cautious with **Attachments**, especially unexpected ones

**M** – Analyse the **Message** for signs of urgency or poor grammar



# Key Learning Point 1 – Appoint a Data Protection Officer

## Importance:

- Oversight and accountability
- Mandatory under PDPA



## Actions:

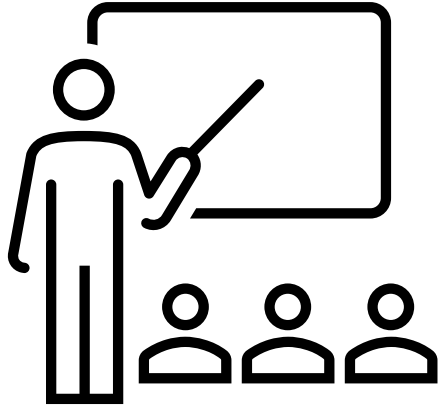
- Appoint and register a DPO
- Provide PDPA and breach handling training



# Key Learning Point 2 – Staff Training

## Train on:

- Phishing awareness
- Safe handling/disposal
- Breach response



## Formats:

- Quarterly quizzes
- Posters



# Key Learning Point 3 – Manage Vendor

## Checklist:

- PDPA compliance?
- Data storage location?
- Audit reports?



## Steps:

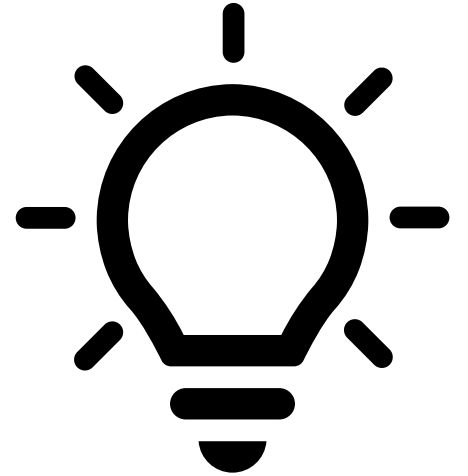
- Vendor risk form
- Maintain vendor log





# Conclusion and Key Takeaways

- Understand your legal obligations under sector-specific Acts
- Appoint and empower your DPO
- Securely store and manage customer identification data
- Secure systems and vendors
- Regularly train staff on handling and protecting personal data
- Maintain cyber hygiene
- Have in place an incident response plan



# Registration Matters and Resources Available



# Reminders on Renewal of Registration (PSMDs)



## Check Your Renewal Period:

- Log in to **myPal** to view your registration validity. Alerts are sent via *myPal* notifications / email reminders / SMS reminders.



## Submit Renewal Application On Time:

- You can renew your registration **90 days** before expiry. Go to the **GoBusiness Dashboard** to complete and submit the renewal application form along with the required registration fee.



If your registration has **expired**, you cannot renew; you will need to submit a new application to become a registered dealer.



It is an **offence** if you act or hold out to be a regulated dealer without being registered or exempted.



# Useful Resources (PSMDs)

## ACD Website

Notice for  
Customers

Sample  
Forms  
(IPPC, RA,  
CDD,  
ECDD)

Compliance  
Toolkit

Video Guides  
(SAR, screening function)

Guidelines  
for  
Regulated  
Dealers

Notices from Registrar



## myPal Portal

Check  
Registration  
Expiry

My  
Notifications

Submit Semi-  
Annual Return

Digital Training  
(CDD, ECDD, STR, CPF)

Survey

Screening Function  
(Perform screening against TSOFA and UN  
sanction lists)



# Useful Resources (Pawnbrokers / Moneylenders)

Registry of Pawnbrokers Website:  
Compliance  
(AML | CFT | CPF)

Red Flag Indicators

AML/CFT/CPF  
Resources

Guidelines for Licensed Pawnbrokers



Registry of Moneylenders Website:  
Compliance  
(AML | CFT | CPF)

Red Flag Indicators

AML/CFT/CPF  
Resources

Guidelines for Licensed Moneylenders



# Thank you!

@minlawsg

