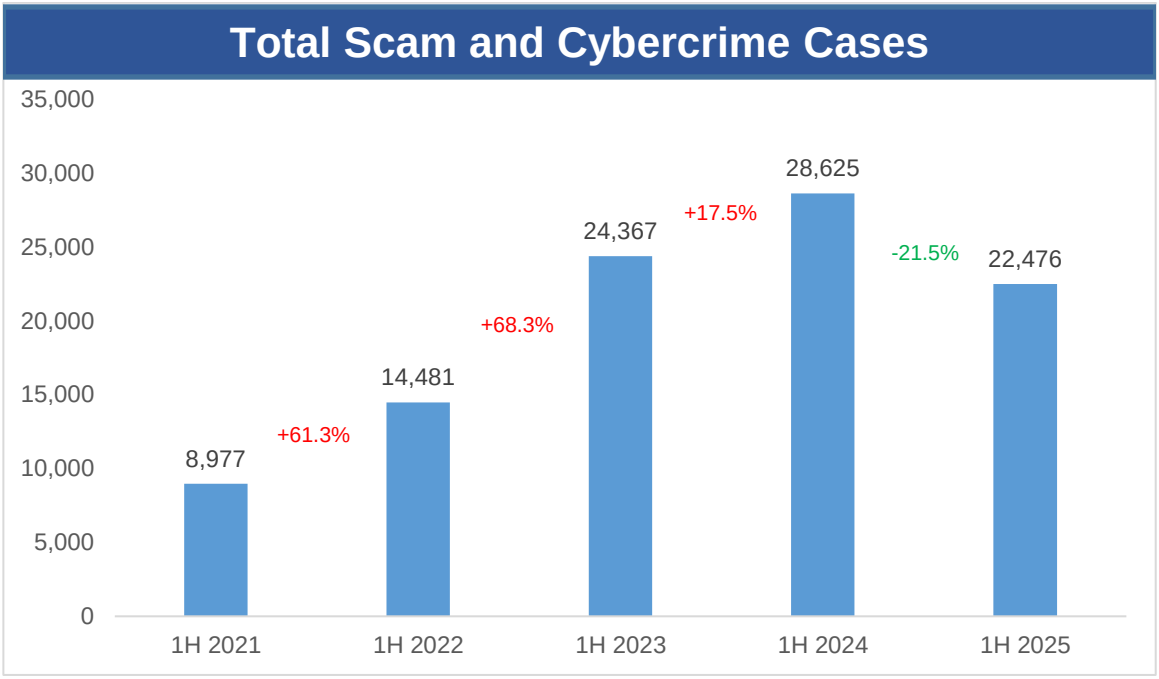
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

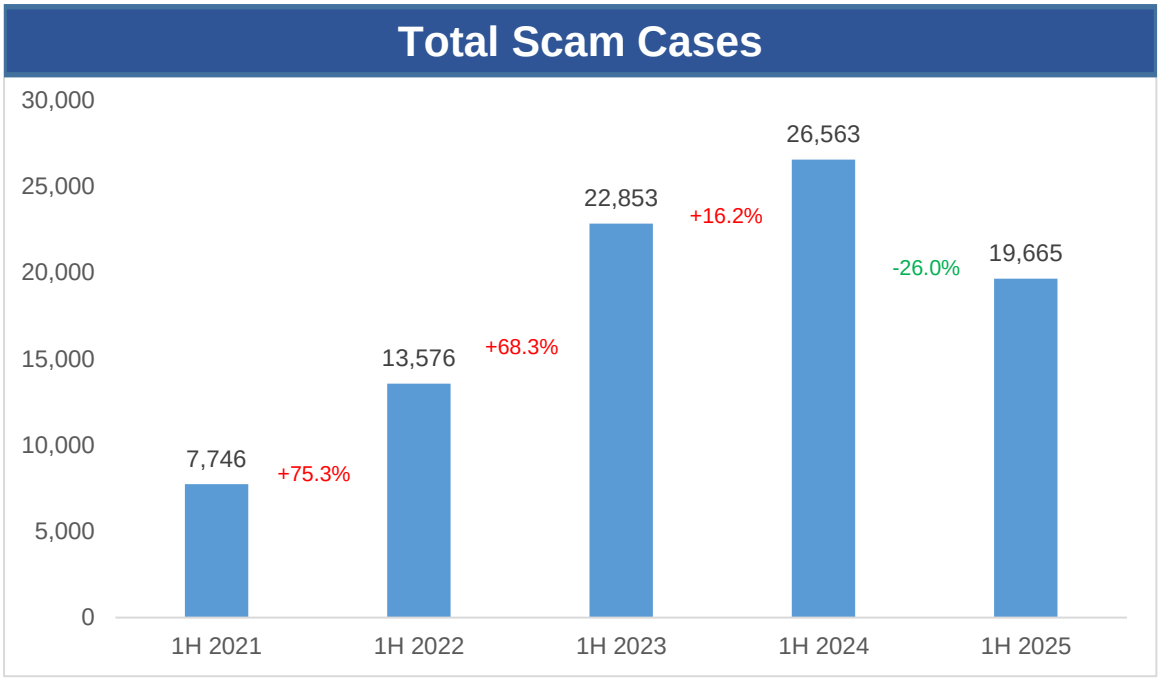
Mid-Year Scam and Cybercrime Brief 2025

Overall Scam and Cybercrime Situation for January to June 2025

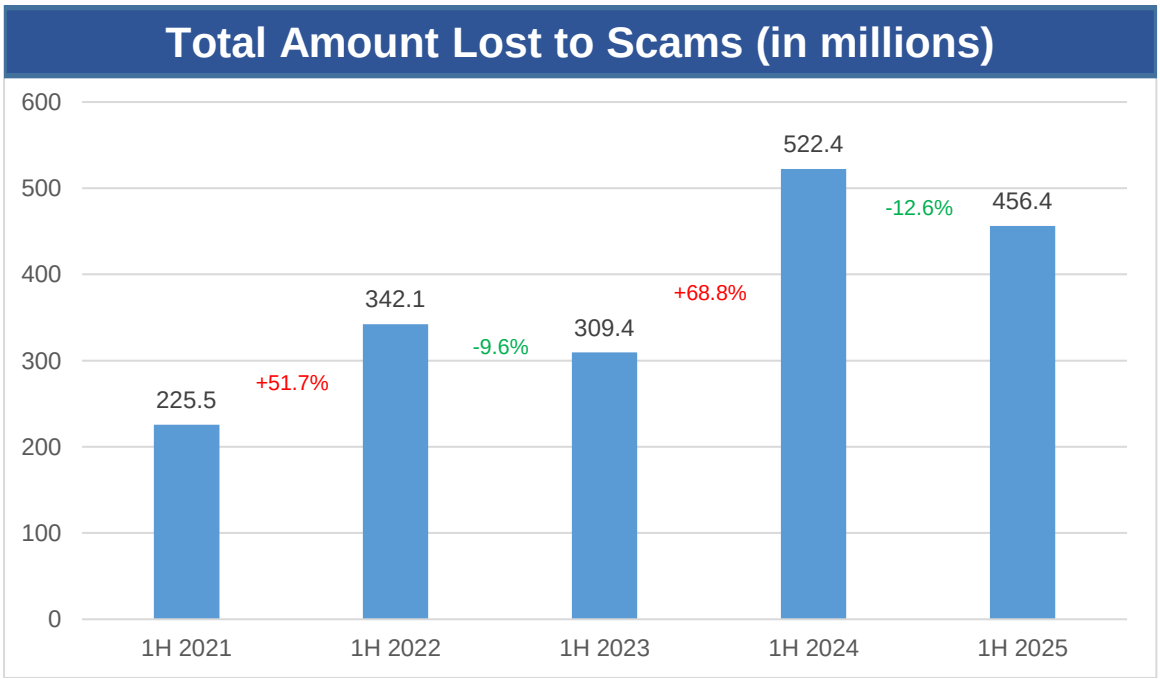
From January to June 2025, the **number of scam and cybercrime cases decreased by 21.5% to 22,476 cases**, compared to 28,625 cases in the same period in 2024.



2. Scams accounted for 87.5% of these 22,476 cases. The **number of scam cases decreased by 26.0% to 19,665 cases in the first half of 2025**, from 26,563 cases in the same period last year.



3. The **amount lost to scams also decreased, by 12.6% to about $456.4 million in the first half of 2025**, from about $522.4 million in the same period last year. **Despite these decreases, the scam situation remains of concern.**

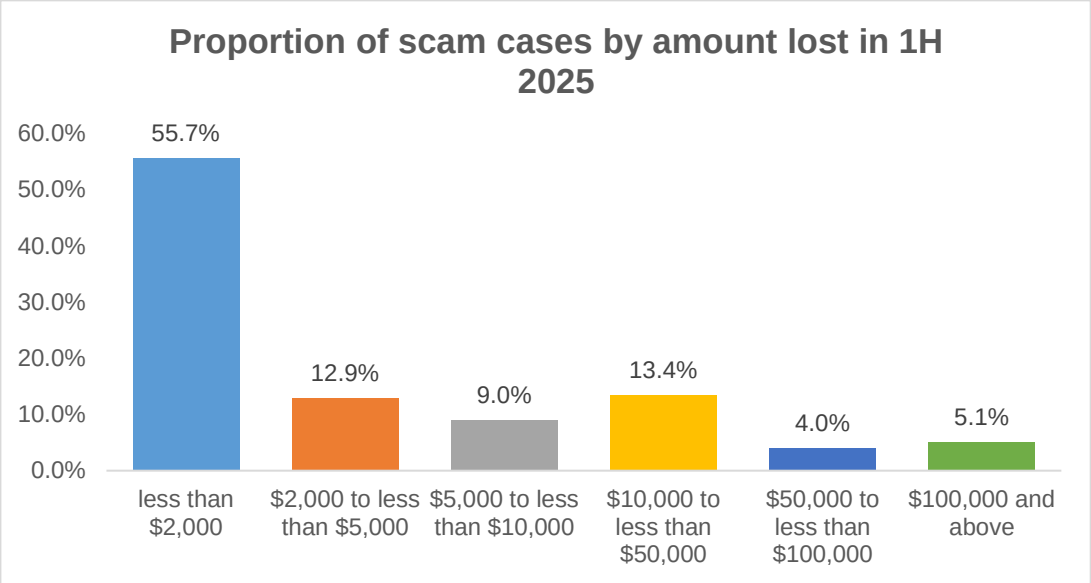


4. In the first half of 2025, the Anti-Scam Command (ASCom) **successfully recovered more than $56.7 million of scam losses**, which includes $39.7 million in

non-cryptocurrency and $17 million in cryptocurrency.[1] In addition, through proactive interventions with victims at various stages of being scammed, ASCom and its partners helped victims **avert at least $179 million in potential losses.**

5. **The majority of scam cases, about 68.6%, saw less than $5,000 in losses**.

6. **The median loss per case increased by 36.4% to $1,500 in the first half of 2025** from $1,100 in the same period in 2024. There was also an **increase in the number of scam cases with losses of at least $100,000** in the first half of 2025, as compared with the same period in 2024 – such cases made up 5.1% of the scam cases in the first half of 2025, and 68.9% of the scam losses; as compared with 2.8% of the scam cases and 70.3% of the scam losses in the first half of 2024.



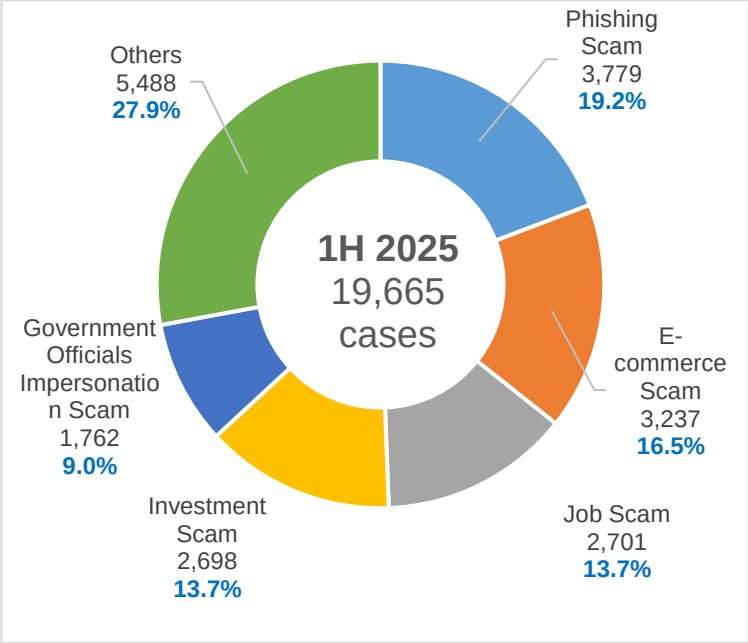
7. The percentage of total reported scams which involved **self-effected transfers** fell to **78.8%** in the first half of 2025, from 86.1% in the same period last year. The decrease may in part be due to the public education efforts, which resulted in increased public vigilance. That said, the number of scams involving self-effected transfers is still high and comprise the large majority of reported scams. In most of the cases, the scammers did not gain direct control of the victims' accounts, but manipulated the victims into performing the monetary transactions by means of deception and social engineering. The Police urge the public to exercise caution when making fund transfers, such as by verifying the legitimacy of such requests beforehand.

[1] The amount of scam losses *recovered* refers to funds in the bank accounts and cryptocurrency wallets of scammers or mules, scammed from victims in cases reported to the Anti-Scam Centre (ASC), that have been frozen by the Police. It does not refer to monies *returned* to scam victims.

Scam and Cybercrime Types of Concern

8. In terms of case numbers, **phishing scams, e-commerce scams, job scams, investment scams and government officials impersonation scams** were the top five scam types in the first half of 2025.

Breakdown of scam types by number of cases

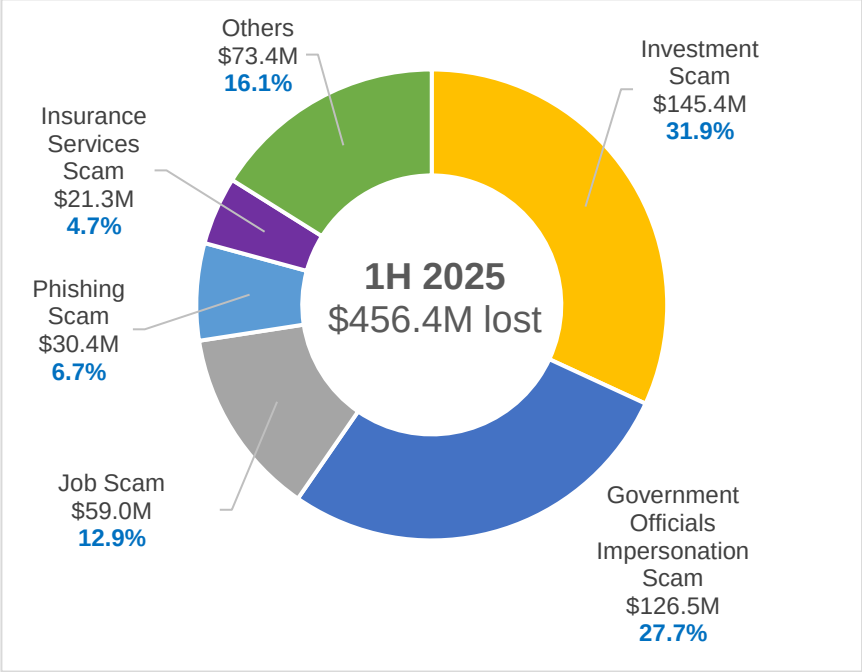


9. In terms of the amount lost, **investment scams, government officials impersonation scams, job scams, phishing scams, and insurance services scams** were the top five scam types in the first half of 2025.

10. **Cryptocurrency losses[2] formed a considerable percentage of scam losses, accounting for about $81.6 million, or about 17.9% of total scam losses in the first half of 2025**. Scammers target cryptocurrency likely due to its irreversible transactions and limited traceability, making asset recovery virtually impossible, unlike traditional banking transactions. **Tether, Bitcoin, and Ethereum** were the top cryptocurrencies that scam victims reported to have lost (details in **Annex B**), and accounted for about 91.2% of total cryptocurrency scam losses.

[2] Cryptocurrency losses refer to the outflow of cryptocurrency from victims' cryptocurrency account or wallet to scammers. It does not include losses where victims transferred money from their bank accounts to fake crypto-investment platforms. It also does not include cases where victims claimed to have incurred cryptocurrency losses but are unable to provide details of the cryptocurrency transactions.

Breakdown of scam types in terms of amount lost (in millions)



11. The key scam types that are of particular concern in the first half of 2025 include:

a) Government officials impersonation scams

i. Government officials impersonation scams remain of concern. **The number of cases reported almost tripled**, increasing by 199.2% to 1,762 cases in the first half of 2025, from 589 cases during the same period in 2024.

ii. At the same time, government officials impersonation scams recorded the second highest loss among all scam types in the first half of 2025. **The amount lost to this scam type increased** by 88.3% to about $126.5 million in the first half of 2025, from about $67.2 million during the same period in 2024.

iii. The Police would like to highlight a rising trend where victims are pressured into withdrawing cash, purchasing gold bars or declaring valuable possessions (e.g. jewellery and luxury watches) before meeting mules in-person to hand over these valuables, purportedly for investigation purposes. Another approach involves fund transfers to credit cards, believed to be done to increase credit limits to enable large purchases of jewellery and precious metals, particularly gold bars.

b) Phishing scams

i. Phishing scams recorded the highest number of reported cases among all scam types in the first half of 2025, with a 10.9% **increase** to 3,779

cases in the first half of 2025, from 3,407 cases during the same period in 2024.

ii. The amount lost to phishing scam cases also **increased significantly,** by 134.0% to about $30.4 million in the first half of 2025, from about $13.0 million during the same period in 2024.

iii. Phishing scams predominantly involve unauthorised card transactions where victims would unknowingly submit their card details and authentication code (via OTP/digital token) to scammers, to complete seemingly legitimate purchases.

c) Investment scams

i. While there was a **decrease** in the number of investment scam cases, by 19.2% to 2,698 cases in the first half of 2025, from 3,338 cases during the same period in 2024, the number of investment scam cases is the fourth highest among all scam types in the first half of 2025.

ii. Notably, the amount lost to investment scams in the first half of 2025, of about $145.4 million, is the highest among the various scam types. This is a 10.6% **increase** from about $131.5 million during the same period in 2024.

d) Insurance services scams

i. Insurance services scam is a **new scam type** that emerged in 2025. There were 791 insurance services scam cases reported in the first half of 2025, with about $21.3 million lost.

ii. Under this scam type, scammers impersonate staff from insurance companies and claim that victims would have to pay for their supposed insurance packages or expiring trial subscriptions, unless they are cancelled. To proceed with the cancellation, victims are asked to verify their identity by sharing personal details and transferring money, with false promises of refunds after verification.

12. **Significant decreases** in both the number of cases reported and amount lost were observed for **job scams, fake friend call scams and e-commerce scams**.

13. Details of the top 10 scam types in Singapore can be found at **Annex C.**

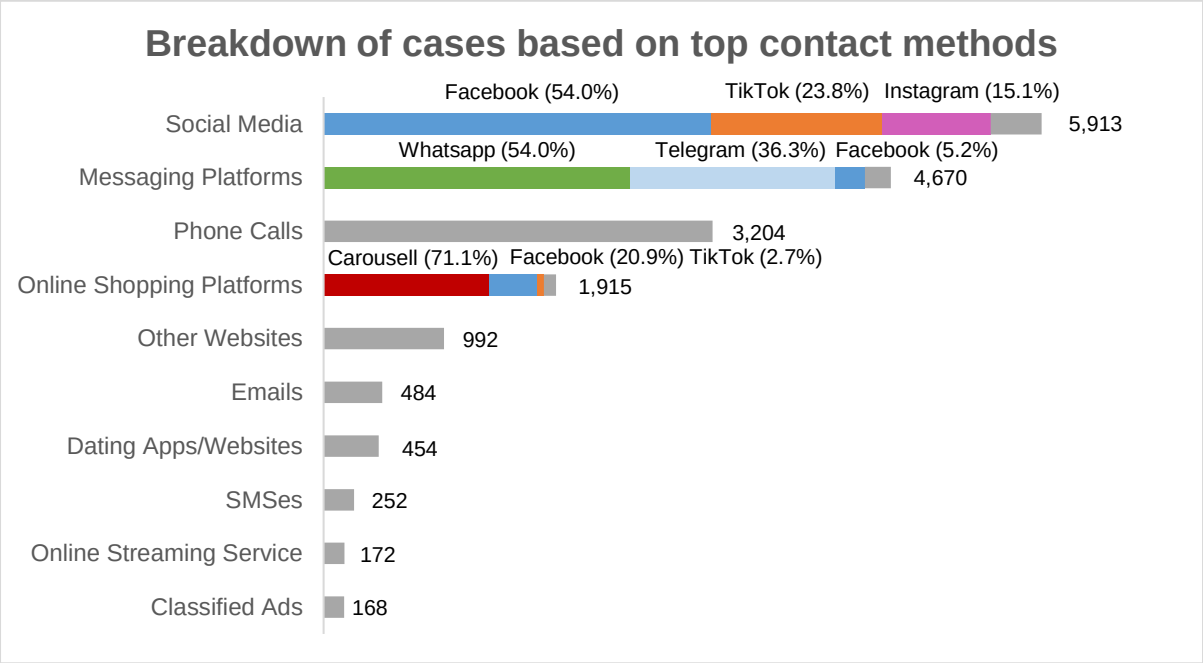
14. A background of the other common or notable scam variants is at **Annex D**.

Top Contact Methods

15. **Social media, messaging platforms, phone calls and online shopping platforms** were the top contact methods which scammers used to reach out to victims.

16. **Three products from Meta (Facebook, WhatsApp, Instagram) remain of particular concern**, as they make up a significant proportion (37.3%) of total cases reported across all platforms exploited by scammers to contact victims. **TikTok, Telegram, and Carousell are platforms of concern too – the number of scam cases perpetrated through TikTok has more than doubled,** and there remains a considerable number of scam cases perpetrated through Telegram and Carousell.

17. More details of the platforms used by scammers can be found at **Annex E**.



Scam Victim Profile

18. **In the first half of 2025, 60.3% of scam victims were youths, young adults, and adults aged below 50.** While the elderly made up a smaller proportion of the scam victims, **there was an increase in the proportion of elderly scam victims**, to 15.0% in the first half of 2025, from 7.2% in the same period in 2024. **The average amount lost per elderly victim was the highest among the various age groups.** The breakdown of scam victims by age group is as follows:

a) **Youths, aged 19 and below, made up 5.5% of scam victims.** 34.6% fell prey to e-commerce scams, while 15.7% fell prey to phishing scams and 13.2% fell prey to job scams. Youths most commonly respond to scammers via messaging

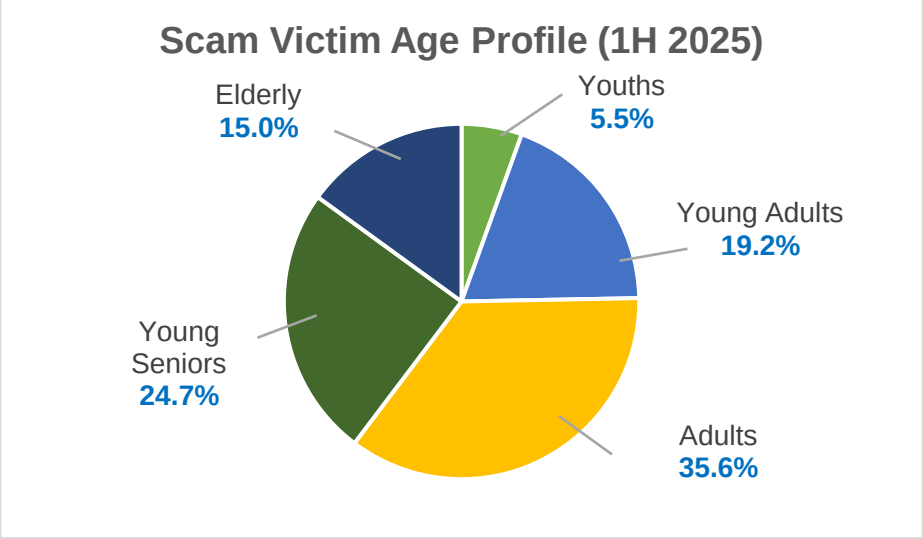
platforms, online shopping platforms and social media. The average amount lost by youths to scams is $4,731 per victim.

b) **Young adults, aged 20 to 29, made up 19.2% of scam victims.** 30.2% fell prey to e-commerce scams, while 17.9% fell prey to job scams and 11.2% fell prey to phishing scams. Young adults most commonly respond to scammers via messaging platforms, social media and online shopping platforms. The average amount lost by young adults to scams is $8,541 per victim.

c) **Adults, aged 30 to 49, made up 35.6% of scam victims.** 20.7% fell prey to e-commerce scams, while 20.2% fell prey to phishing scams and 15.8% fell prey to job scams. Adults most commonly respond to scammers via social media, messaging platforms and phone calls. The average amount lost by adults to scams is $22,329 per victim.

d) **Young seniors, aged 50 to 64, made up 24.7% of scam victims.** 25.6% fell prey to phishing scams, while 16.4% fell prey to investment scams and 12.7% fell prey to government officials impersonation scams. Young seniors most commonly respond to scammers via social media, messaging platforms and phone calls. The average amount lost by young seniors to scams is $29,434 per victim.

e) **The elderly, aged 65 and above, made up 15.0% of scam victims.** 21.1% fell prey to investment scams, while 19.7% fell prey to phishing scams and 18.8% fell prey to government officials impersonation scams. Elderly most commonly respond to scammers via social media, phone calls and messaging platforms. The average amount lost by the elderly to scams is $33,672 per victim.



Police's and Whole of Government Efforts to Fight Scams and Cybercrimes

19. The SPF continues to work closely with Government agencies and private sector stakeholders to strengthen scam intervention measures to minimise victims' losses, and share information to prevent scams.

20. Some of the **recently implemented and key anti-scam initiatives by the SPF** (more details at **Annex F**) include:

- Operationalisation of the **Protection from Scams Act** on 1 July 2025, with two Restriction Orders issued as of 20 August 2025.
- Operationalisation of the Anti-Scam Centre (ASC)'s **Crypto Tracing Team (CTT)** in March 2025, to address the emerging threat of scam proceeds being rapidly dissipated via cryptocurrencies.
- **Addition of GXS Bank to the list of partners co-located at the ASCom** in March 2025.
- **Steady increase in the usage of anti-scam resources** (ScamShield app, ScamShield website, 24/7 ScamShield Helpline, ScamShield Alert social channels) by the public, since the launch of the ScamShield Suite. In particular, the ScamShield Helpline receives around 500 to 700 calls daily, where around 80% of callers called in to check if something is a scam, and the helpline operators would assist them in avoiding being scammed.
- **Ramped up enforcement efforts against those who abuse local SIM cards to perpetrate scams**, following the operationalisation of offences targeting the misuse of SIM cards on 1 January 2025.

21. Other **recently implemented and upcoming anti-scam initiatives by other government agencies** (more details at **Annex G**) include:

- Expansion of the Shared Responsibility Framework (SRF) by the **Monetary Authority of Singapore (MAS)** to include a **new fraud surveillance duty** – which detects rapid withdrawals of large sums from customer accounts. MAS is also working with banks on a **Fast IDentity Online (FIDO)-compliant hardware token** that must be inserted into a customer's device to approve higher value internet banking payments and transfers.
- Provision of technical expertise by the **Cyber Security Agency of Singapore (CSA)** in a joint operation between the SPF, Hong Kong Police Force (HKPF) and Royal Malaysia Police (RMP) from April to June 2025, that **disrupted a**

criminal syndicate operating Voice over Internet Protocol (VoIP) GSM gateway devices for scam calls. CSA will launch its **sixth National Cybersecurity Campaign** in September 2025.

- Creation of '**Unpacked**' by the **Open Government Products (OGP)**, which is an immersive, mobile-first simulation that allows users to experience a scam firsthand to better understand how it unfolds.
- **All telecommunications companies in Singapore now offer customers the option to block incoming international calls and SMSes on mobile and residential fixed lines**. The **Infocomm Media Development Authority (IMDA**) has also been working with telecommunications companies to detect and act against the suspected misuse of local mobile numbers based on suspicious traits.
- Consolidation of all outbound calls by the **Central Provident Fund Board (CPFB)** into a single number in April 2025. **All calls from the CPFB will only be made from 6227 1188.**

Everyone Plays a Part in Fighting Scams

22. Everyone has a part to play in keeping Singapore safe and secure. Individuals should proactively adopt anti-scam measures to enhance their resilience against scams. When in doubt, they are encouraged to check with someone they trust, call the ScamShield Helpline at 1799, or check the ScamShield app.

23. Criminal syndicates are perpetrating scams in Singapore by using local mules. Members of the public should be wary not to become a mule, whether deliberately for financial gain, or allow themselves to be inadvertently used. This includes allowing scammers to use their payment accounts such as bank accounts to move criminal proceeds, to use their Singpass account, or to supply scammers with local SIM cards. Your payment accounts, Singpass account, and SIM cards are for your own use only. A person convicted of mule-related offences may be liable for significant imprisonment terms and fines.

24. In the first half of 2025 alone, more than 3,500 money mules and scammers suspected to be involved in scam cases were investigated, of whom more than 500 have been charged by the Police so far. We will continue to come down hard on people who commit or facilitate the commission of scams.

25. Business operators, particularly banks, online marketplaces and telcos, have a responsibility to prevent, deter and detect crimes committed through their platforms. Putting in place anti-scam measures and precautions will help keep their customers safe.

26. The Government will continue to work on safeguards and measures to make it harder for scammers to target Singaporeans. The Government will also continue rolling out extensive anti-scam public education, to empower members of the public with the knowledge, skills and tools to guard against scams.

27. Please see **Annex A** for comments by Mr Goh Pei Ming, Minister of State, Ministry of Home Affairs & Ministry of Social and Family Development.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
30 AUGUST 2025 @ 3PM

Annex A

Quote by Minister of State (MOS) for Home Affairs and Social and Family Development

“Although overall scam cases and losses decreased in the first half of 2025, scams and cybercrime remain a persistent and serious threat to Singaporeans. Scammers have continued to adapt their methods and target our vulnerabilities, as demonstrated by the increases in phishing and government officials impersonation scams, and the higher median losses per case. That said, the significant reductions in job scams, fake friend call scams and e-commerce scams reflect the impact of the Government’s enforcement, education and engagement efforts. Therefore, we need to strengthen our defences and pursue scammers relentlessly, and keep up with our public education and engagement efforts. Every member of the public must also remain alert to scam tactics and take personal responsibility to safeguard themselves and their families.”

- MOS Goh Pei Ming

Annex B

Top 5 Cryptocurrencies Lost to Scams in 1H 2025

(Based on estimated value in Singapore dollars)

Cryptocurrency	Cryptocurrency units lost	Estimated value in Singapore dollars (approximate)
Tether	35,453,536.53	$46.8M
Bitcoin	150.81	$20.0M
Ethereum	2,348.56	$7.6M
USD Coin	4,084,281.85	$5.3M
XRP	125,296.09	$386K

Annex C

Top 10 Scam Types in Singapore
(Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (approximate)		Average amount lost in 1H 2025
	1H 2025	1H 2024	1H 2025	1H 2024	
Phishing Scams	3,779	3,407	$30.4M	$13.0M	$8,057
E-commerce Scams	3,237	7,224	$7.6M	$8.5M	$2,353
Job Scams	2,701	5,753	$59.0M	$84.2M	$21,861
Investment Scams	2,698	3,338	$145.4M	$131.5M	$53,915
Government Officials Impersonation Scams	1,762	589	$126.5M	$67.2M	$71,842
Fake Friend Call Scams	1,053	2,370	$2.8M	$7.8M	$2,689
Insurance Services Scams	791	-	$21.3M	-	$27,004
Sexual Services Scams	553	563	$1.4M	$2.1M	$2,654
Loan Scams	457	581	$3.0M	$2.5M	$6,660
Internet Love Scams	433	410	$12.0M	$12.8M	$27,920
Top 10 scams	**17,464**	**24,235**	**$409.9M**	**$329.9M**	**$23,474**

Note: Total scam losses may not tally due to the rounding of figures.

Annex D

Background Information on Common or Notable Scam Variants

Government Officials Impersonation Scams

- The majority of government officials impersonation scam victims were aged 50 to 64, comprising 34.8% of victims for this scam type. Phone calls and WhatsApp were the most common channels used by government officials impersonation scammers to contact potential victims.

- Government officials impersonation scams typically involve scammers impersonating local government officers (e.g. SPF, Immigration & Checkpoints Authority (ICA), MAS), bank or financial institution representatives (e.g. Unionpay, NTUC), or China government officials (e.g. China Police). The notable variants include the following actions by scammers:

    - **Impersonation of bank or financial institution representatives and local government officials through calls** – Victims typically receive unsolicited calls from scammers impersonating representatives from banks or financial institutions (e.g. Unionpay, NTUC), who would cite or seek verification on banking or financial transactions supposedly allegedly conducted by victims (e.g. transactions made on credit card applied by victim, insurance policy with victim's details that was due for payment or renewal). When victims denied making such transactions or possessing such bank cards, they would be transferred to another scammer claiming to be a government official (e.g. SPF, MAS), who would accuse victims of being involved in criminal activities, such as money laundering. Scammers would then instruct victims to perform monetary transactions for investigation or safekeeping purposes, such as transferring money to bank accounts (or 'safety accounts') purportedly designated by the government, or handing over cash to unknown subjects. This variant accounted for 93.4% of the total cases in the first half of 2025.

    - **Impersonation of China government officials (e.g. China Police) and local government officials through calls** – Victims typically receive unsolicited calls from scammers impersonating government officials (e.g. ICA) or at times representatives from airlines and telecommunication companies, who would claim that victims were associated with credit cards, bank accounts, phone numbers or flight ticket purchases that were eventually involved in fraudulent activities, such as the sending of scam messages. When victims denied being involved, they would be transferred to another scammer claiming to be a China government official (e.g. China Police), who would accuse

victims of being involved in criminal activities, such as money laundering. Scammers would then instruct victims to perform monetary transactions for investigation or bail purposes, such as transferring money to bank accounts (or 'safety accounts') supposedly designated by China authorities or handing over cash to unknown subjects. This variant accounted for 6.6% of the total cases in the first half of 2025.

- The Police would like to highlight a rising trend where victims are pressured **into withdrawing cash, purchasing gold bars or declaring valuable possessions (e.g. jewellery and luxury watches) before meeting cash mules in-person** to hand over these valuables, purportedly for investigation purposes. Apart from government officials impersonation scam, the handing over of valuables to scammers is also seen in other scam typologies including **investment scam and job scam**.

- The Police have also observed a **new money transfer method involving fund transfers to credit cards**, in both **government officials impersonation scam and insurance services scam**. Since May 2025, there has been a pattern of scammers instructing victims to make fund transfers from their bank accounts to credit cards provided by the scammers. These transfers were believed to be done to increase credit limits, enabling large purchases of jewellery and precious metals, particularly gold bars.
- The Police would like to remind members of the public that they should NEVER transfer monies, hand monies or other valuables to any unknown persons or persons whose identity you did not verify. NEVER place monies or valuables at a physical location to facilitate subsequent collection.
- We would also like to inform members of the public that Singapore Government officials will never ask members of the public to do the following over a phone call:
    - Ask you to transfer money;
    - Ask you to disclose banking log-in details;
    - Ask you to install mobile apps from unofficial app stores;
    - Transfer your call to Police

<u>Investment Scams</u>

- The majority of investment scam victims were aged 30 to 49, making up 35.1% of victims for this scam type. The most common platforms which scammers used to contact investment scam victims were Telegram and Facebook.

- Victims of investment scams came across "investment opportunities" through recommendations from online friends, from their own internet searches, or were

added into chatgroups or channels via messaging platforms by scammers purportedly for "investment opportunities". Some victims also received unsolicited messages from scammers offering "investment opportunities". Once they were duped or had been enticed by the false testimonies, victims would either follow the scammers' instructions to transfer monies to specified bank accounts or cryptocurrency wallets, or make payments via their bank cards for the purpose of investing.

- Scammers have also directed victims to **create new cryptocurrency wallets** for their "investment". Victims are then instructed to fund their wallet with money or cryptocurrencies. Some victims **transfer the funds directly to scammer-controlled wallets or link their cryptocurrency wallet to the fraudulent investment websites** for their "investment". In some cases, victims **share their login** credentials (e.g. seed phrase) with scammers after trust is established, which allows the scammers to gain access and drain the funds from the wallet.

- Victims would discover that they had been scammed when they experience difficulties withdrawing their earnings from their "investments" despite transferring increasingly large sums of "fees" incurred for the "investment".

- In some instances, the victims would receive initial small "profits" which led them to believe that their "investments" were genuine, enticing them to invest more money by transferring larger amounts of monies or cryptocurrencies to the scammers. "Investment" websites or applications displaying alleged growing "profits" earned by victims would also lead them into investing larger sums.

- Members of the public are strongly advised to be cautious when responding to investment advertisements and when making investment decisions. Members of the public should only deal with regulated entities and representatives as listed on the Financial Institutions Directory and Financial Institution Representatives Register (FIRR) on MAS' website. Verify the identity of the person promoting the investment by meeting him/her in person at the financial institution's premises, matching the name on his/her official ID against the FIRR, and checking his/her appearance against the official ID. Investors should be wary of red flags when considering investment "opportunities", such as guaranteed or high returns at little or no risk, or pressure to act urgently citing time-limited offers.

Phishing Scams

- The majority of phishing scam victims were aged 30 to 49, comprising 36.9% of victims for this scam type. Facebook and TikTok were the most common channels used by phishing scammers to contact potential victims.

- Phishing scams involve emails, text messages, calls, or advertisements from scammers posing as government officials, financial institutions or businesses. Victims would be tricked into revealing sensitive information such as banking credentials and/or debit or credit card information after clicking malicious links or via phone calls. Upon acquiring the victims' information, scammers would perform unauthorised transactions on the victims' bank accounts or debit/credit cards.

- In the phishing scam variants, victims would discover that they had been scammed when they found unauthorised transactions made from their bank accounts or debit/credit cards. Some phishing scam variants include the following:

    - Victims usually encounter **enticing deals** (e.g. heavily discounted transport cards, food-related advertisements) **on social media platforms** (e.g. Facebook, TikTok, Instagram) that lead them to fraudulent phishing links. Victims would unknowingly submit their card details and authentication (OTP/Digital Token) to scammers, to complete the seemingly legitimate purchases. In the first half of 2025, there were 1,930 cases where social media advertisements were used to lure victims into clicking on phishing links, with total amount lost amounting to $3.1 million. The compromised card credentials are then misused in three ways:

        a. Addition to scammer-controlled mobile wallets (e.g. Apple Pay, Google Pay, Samsung Pay) for both in-store NFC purchases and online transactions, particularly on e-commerce and cryptocurrency platforms

        b. Direct use of card details for online purchase

        c. Linking to payment services and e-wallets (e.g. Grab, YouTrip, Revolut) for unauthorised top-ups and transactions

    - Victims would receive **unsolicited phone or in-app calls allegedly from government officials** such as the SPF, Ministry of Manpower, or the MAS. Scammers would claim that there were issues with victims' bank accounts or that they require the victims' details for purposes of investigation or further verification. Victims would then be convinced to

disclose their banking credentials, debit/credit card details, personal details, and/or OTPs/perform digital authentication.

- Members of the public are advised to be prudent when making online payments and to visit only reliable websites for online shopping. They should also opt for SMS notifications to be sent to their mobile phone for any charges incurred on your credit or debit cards, and regularly check their bank statements and alert the bank immediately should there be any discrepancies or unauthorised charges. When making payment online, buyers should read the notifications sent and be clear of what they are approving, before providing OTP or approve digital tokens.

Insurance Services Scams

- The majority of insurance services scam victims were aged 65 and above, comprising 27.6% of victims for this scam type. Phone calls and WhatsApp were the most common channels used by insurance services scammers to contact potential victims.

- In this scam type, scammers would typically pose as insurance service representatives (e.g. UnionPay, NTUC) and claim that victims have insurance packages purchased or expiring trial subscriptions. They would claim that fees will be automatically deducted unless these packages or subscriptions are cancelled. To proceed with the cancellation, victims would have to verify their identities and bank accounts, by providing their personal information and making monetary transfers to bank accounts provided by scammers. The victims were assured that their monies would be refunded upon successful verification.

- In some cases, the scammer would guide the victim through WhatsApp's screen sharing function to increase the bank transaction limit and to perform the bank transfers. There were also cases where scammers impersonated government officials (e.g. MAS) to assist victims in the cancellation of the purported insurance package. Most victims would only realise that they had been scammed after making multiple monetary transfers without receiving the promised refunds.

E-commerce Scams

- E-commerce scams saw a significant decrease in the number of cases reported in the first half of 2025, by 55.2% to 3,237 cases, from 7,224 cases in the first half of 2024. Despite so, e-commerce scams recorded the second highest number of reported cases among all scam types in the first half of 2025. The total amount lost to e-commerce scams also decreased, by 10.7% to about $7.6

million in the first half of 2025, from about $8.5 million during the same period last year.

- The majority of e-commerce scam victims were aged 30 to 49, making up 43.6% of victims for this scam type. The most common platforms which scammers used to contact e-commerce scam victims were Carousell and Facebook.

- E-commerce scams typically involve the sale of goods and services without physical meet-ups. Generally, victims would come across attractive deals on online marketplaces or social media platforms but would fail to receive the goods or services after making payment. In some cases, the victims could also be sellers who did not receive payment after delivering the goods or services to scammers pretending to be buyers. The scammers sometimes provided victims with fake screenshots as “proof of payment”.

- Concert tickets were the top item involved in e-commerce scams, with related cases accounting for 14.4% of the total e-commerce scam cases in the first half of 2025, as compared to 28.4% in the same period in 2024. Victims typically came across concert ticket listings online and were asked to transfer payments. In some cases, victims received the tickets, but only realised that they were fake when they were unable to use them to enter the concert venue. Since 2024, concert ticket scams have pivoted to messaging platforms such as Telegram, where interventions and disruption efforts are harder compared to traditional e-commerce marketplaces.

Job Scams

- There was a marked decrease in the number of job scams reported in the first half of 2025, by 53.1% to 2,701 cases, from 5,753 cases in the first half of 2024. The total amount lost to job scams in the first half of 2025 also saw a decrease, by 29.9% to about $59.0 million in the first half of 2025, from about $84.2 million during the same period last year. However, the total amount lost from job scams in the first half of 2025 was the third highest among all scam types.

- The majority of job scam victims were aged 30 to 49, making up 41.0% of victims for this scam type. The most common platforms which scammers used to contact job scam victims were WhatsApp and Facebook.

- Job scams typically involve victims being offered online jobs that could be performed from home. Victims chance upon “job opportunities” through social media platforms like Facebook, TikTok, Instagram or through their own internet searches. Victims would also be contacted by scammers for job offers via messaging platforms such as WhatsApp and Telegram or be added into chatgroups or channels of these messaging platforms. Victims would be asked

to perform simple tasks for a commission, such as booking or reviewing hotels/restaurants/airlines, making advance purchases, completing surveys, “boosting” value of cryptocurrencies, “boosting” ratings of product listings for online merchants, “rating” mobile apps to improve their rankings on app stores, or liking or following social media posts or accounts. Victims would initially receive commissions for these “jobs” but would eventually be requested to pay to complete more tasks to earn more commissions. The victims would eventually realise that they had been scammed when they failed to receive their commission, when they were unable to withdraw the monies, or when the scammers could no longer be contacted.

- In the first half of 2025, a notable job scam variant involved victims being asked to start their own business by running an online store. Victims may be asked to register accounts on fake websites or applications. Whenever an order is received via the online store, victims would be required to put in their own money to purchase the orders and will earn a commission once orders are delivered. Initially, the victims may receive the commission as promised. The orders received would require increasingly larger sums of money from the victims, and in the process of completing the orders or despite the completion of the orders, they would be informed of certain issues that require them to put in more of their own money before they can withdraw their funds. This variant could be highly convincing as victims will see an increase in their funds online, prompting them to put in more funds with the hopes of higher returns.

- In other cases, scammers would befriend victims online and ask for assistance in their part-time jobs or offer opportunities to earn money. Victims would be provided legitimate e-commerce websites and asked to screenshot specific products and make advance payments to fake “business accounts” to receive commissions with promised refunds. This process would be repeated several times, beginning with low-cost items, before progressing to more expensive ones. Victims would initially receive commissions and refunds, but the scammers would eventually claim to have encountered issues and stop “paying” victims before becoming uncontactable.

Fake Friend Call Scams

- Fake friend call scams saw decreases in both number of cases reported and amount lost in the first half of 2025. The number of fake friend call scam cases decreased by 55.6% to 1,053 cases in the first half of 2025, from 2,370 cases in the first half of 2024, and the total amount lost also decreased, by 64.0% to about $2.8 million in the first half of 2025, from about $7.8 million during the same period last year.

- The majority of fake friend call scam victims were aged 30 to 49, making up 32.2% of victims for this scam type. The most common platforms which

scammers used to contact fake friend call scam victims were phone calls and WhatsApp.

- Fake friend call scams typically involve scammers contacting victims via phone calls or WhatsApp, prompting victims to guess their identity, then conveniently assume the name provided by the victim. During the conversation, the scammers would claim that they have lost their mobile phone and/or changed phone number. After establishing rapport, scammers would capitalise on the perceived friendship and seek money from the victims for various reasons. The common reasons offered by scammers for these “loans” were to pay hospital fees, pay contractors for renovation fees, pay vendors/suppliers, or issues with PayNow/iBanking. Scammers would provide PayNow numbers for victims to make the transfers. Victims typically discover that they had been scammed only after contacting their real friends or when promised repayments fail to materialise.

Malware-Enabled Scams

- The number of malware-enabled scam cases saw a sharp rise by 266.7%, with 363 cases reported in the first half of 2025, up from 99 cases reported in the same period in 2024. The total amount lost to malware-enabled scams in the first half of 2025 however, decreased by 95.6% to about $5.5 million, from about $125.4 million in the same period in 2024.

- The majority of malware-enabled scam victims were aged 50 to 64, comprising 43.3% of victims for this scam type. Facebook and TikTok were the most common channels used by malware-enabled scammers to contact potential victims.

- In the first half of 2025, there was a resurgence of malware-enabled scams, which saw scammers abusing the Android Debug Bridge (ADB) function to perpetrate scams. Designed as a developer tool to facilitate debugging of Android applications by connecting computers to Android devices, ADB was exploited by scammers to gain unauthorised remote access to victims’ mobile devices. In response, banks promptly enacted measures to address this threat. Members of the public are strongly advised not to turn on the ADB function on their Android devices.

Annex E

Top Contact Methods

Social Media Platforms

- In the first half of 2025, while social media platforms were the most common means by which scammers contacted victims, there was a **decrease** in the number of scam cases by 23.5% to 5,913 in the first half of 2025, from 7,726 in the same period in 2024. In particular, 54.0% were contacted through Facebook, 23.8% were contacted through TikTok, and 15.1% through Instagram. Of the scam cases in the first half of 2025 involving social media platforms**, majority of the cases (69.1%)** were on **Meta platforms** (i.e. Facebook and Instagram).

Messaging Platforms

- Similarly, the number of scam cases where scammers contacted victims via messaging platforms **decreased** by 44.1% to 4,670 in the first half of 2025, from 8,358 in the same period in 2024. In particular, 54.0% were contacted through WhatsApp, 36.3% were contacted through Telegram and 5.2% were contacted through Facebook Messenger. The number of scam cases perpetrated on Telegram also saw a **decrease** of 55.2% in the first half of 2025, to 1,693 cases.

Phone Calls

- Phone calls remain a contact method of concern. There was a 16.0% **increase** in the number of scam cases perpetrated via this platform, to 3,204 in the first half of 2025, from 2,763 in the same period in 2024.

Online Shopping Platforms

- Online shopping platforms is another contact method of concern. There was however a 34.5% **decrease** in the number of scam cases perpetrated via this platform, to 1,915 in the first half of 2025. from 2,922 in the same period in 2024. In particular, 71.1% of these cases occurred on Carousell, 20.9% on Facebook Marketplace and 2.7% on TikTok Shop.

Annex F

Police's Efforts to Fight Scams and Cybercrime

Enforcement

Strengthening legislative levers

Operationalisation of the Protection from Scams Act 2025

The Protection from Scams Act 2025 was enacted by Parliament on 7 January 2025 and came into effect on 1 July 2025. The Act empowers the Police to issue a Restriction Order (RO) to banks to restrict the banking transactions of an individual if there is reason to believe that the individual is likely to make money transfers to a scammer. The Act enables the Police to have legal powers to intervene decisively when victims remain unconvinced of being scammed to prevent further losses, and gives the Police more time to engage and convince the individual that he or she is being scammed.

2. As of 20 August 2025, two ROs have been issued by the Police to banks to restrict the banking transactions of two individuals.

Law enforcement interventions and operations

Operationalisation of the Crypto Tracing Team (CTT)

3. To address the emerging threat of scam proceeds being rapidly dissipated via virtual assets, the ASC operationalised the CTT in March 2025 and established partnerships with over 10 stakeholders, including digital payment token service providers, major payment institutions, and stablecoin issuers. The CTT strengthens the ASC's capabilities to trace, freeze, and recover scam-tainted virtual assets through real-time blockchain analysis and coordination with local and overseas exchanges, stablecoin issuers, and blockchain analytics platforms.

Enforcement operations against scammers and money mules

4. In the first half of 2025, the ASCom, together with the Scam Strike Teams (SSTs) in the seven Police Land Divisions, conducted 13 island-wide anti-scam enforcement operations, leading to the investigation of more than 3,500 money mules and scammers, suspected to be involved in scam cases involving losses of over $123 million. Police have charged more than 500 of these scammers and money mules in Court, including more than 280 of them under the amended laws of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Computer Misuse Act (CMA).

Enforcement operations to combat scams with high losses

5. To combat scams with high losses, particularly government officials impersonation scams, investment scams and job scams, the ASCom together with the SSTs in the seven Police Land Divisions, conducted a series of targeted operations to disrupt and dismantle the scammers' mule account network, infrastructure and communication channels used to contact victims. The Police conducted five operations, which resulted in the freezing of more than 1,750 bank accounts involving over $7.6 million in suspected scam proceeds, terminated more than 6,600 phone lines and 4,400 online social media enablers, arrested 122 persons and investigated another 234 persons for their alleged involvement in money mule activities.

Enforcement operations against the misuse of SIM cards

6. Since the operationalisation of the offences targeting the misuse of SIM cards under the Miscellaneous Offences Act on 1 January 2025, the Police have ramped up enforcement efforts against those who abuse local SIM cards to perpetrate scams. In the first half of 2025, the ASCom along with the seven Police Land Divisions conducted three operations, which resulted in the termination of over 3,500 mobile lines, arrest of 93 persons and the investigation of another 119 persons for their suspected involvement in providing fraudulently registered postpaid SIM cards for monetary gains. Of the arrests made, one recruiter was also arrested for his suspected involvement in sourcing potential SIM card abusers, receiving SIM cards from subscribers who had errantly subscribed to postpaid SIM cards and making payment to them.

Partnerships to disrupt online criminal content and activities and enforce against scams

7. In the first half of 2025, the SPF disrupted more than 58,700 mobile lines, more than 33,300 WhatsApp lines, more than 21,600 online monikers and advertisements, and more than 30,200 websites that were scam-related. This is a significant increase in disruptions as compared to the first half of 2024, and was done through collaborations with other government agencies such as the HTX (Home Team Science & Technology Agency), GovTech Singapore and IMDA, as well as major industry stakeholders such as Meta, Carousell, Google and the telecommunications companies.

Disrupted asset	1H 2024	1H 2025	% increase
Mobile lines	> 16,900	> 58,700	> 245%
WhatsApp lines	> 14,900	> 33,300	> 122%

Online monikers and advertisements	> 13,400	> 21,600	> 60%
Websites	> 18,500	> 30,200	> 63%

8. The ASCom partners with more than 150 institutions, including financial institutions, card security groups, fintech companies, cryptocurrency houses, remittance service providers, INTERPOL and overseas law enforcement agencies from jurisdictions such as Hong Kong SAR and Malaysia, to facilitate the swift freezing of accounts and recovery of funds and mitigate victim losses. This is achieved through establishing direct communication channels with these partners. **In the first half of 2025, the ASCom froze more than 8,600 bank accounts based on reports referred to the ASC and successfully recovered more than $39.7 million. Another $17 million in cryptocurrency was recovered, making up a total recovery of $56.7 million.**

9. The co-location initiative was also expanded to include the **co-location of GXS Bank** in March 2025. This initiative was instrumental in supporting ASCom in proactive detection of scam-tainted bank accounts and swift fund recovery.

Collaboration with foreign law enforcement agencies

10. Most online scams are perpetrated by scammers based outside of Singapore, making such cases difficult to investigate and prosecute. The SPF continues to foster international cooperation to tackle the transnational nature of scams, to enhance cross-border asset recovery and tighten collaboration efforts.

Takedown of scam syndicates through collaboration with overseas law enforcement agencies

11. In the first half of 2025, the close collaboration between the SPF and overseas law enforcement agencies resulted in the successful takedown of eight transnational scam syndicates comprising one fake friend call syndicate, two suspected money laundering cells, one government officials impersonation scam call centre and four syndicates hosting gateway devices and Simpools used to perpetrate scam calls. The coordinated efforts resulted in the arrest of over 36 persons based overseas and 111 persons based locally who were responsible for more than 764 transnational scam cases involving losses of more than $3 million.

12. **Fake friend call scams recorded a decrease of 55.6% in the number of cases reported.** There is also a **64.0% decrease in losses in the first half of 2025**, as compared to the same period in 2024. This can in part be attributed to the continued collaboration between the SPF, foreign law enforcement agencies and local government agencies in dismantling scam syndicates.

- Since 2024, the SPF and the RMP have dismantled five fake friend call scam syndiates operating in Malaysia. The latest syndicate was busted in Johor Bahru Malaysia on 14 April 2025, resulting in the arrest of 10 syndicate members and seizure of more than 30 mobile phones.

- Between April and June 2025, the ASCom, in collaboration with the CSA, IMDA, RMP and HKPF, conducted several operations against a transnational scam syndicate. The syndicate had employed an advanced cloud-based remote operating system, enabling them to link to Voice over Internet Protocol (VoIP) GSM mobile phone networks across the three jurisdictions. This arrangement allowed the syndicate to operate remotely and route fraudulent calls through our local mobile phone networks, leading victims in Singapore to believe that they were receiving calls from within Singapore. 11 suspects were arrested across the three jurisdictions, and more than 200 GSM gateway devices were seized. The syndicate is believed to be linked to more than 480 cases of government officials and Chinese services impersonation scams, with losses exceeding $3.1 million. These series of operations have been effective in crippling the scammers' communication infrastructure, slowing their reach to potential victims.

International cooperation for asset recovery

13. Since the formalisation of **"FRONTIER+"** in October 2024, involving the anti-scam units of six jurisdictions, namely Singapore, Hong Kong SAR, Thailand, the Republic of Korea, the Republic of Maldives and Malaysia, this initiative has **expanded to a total of 11 jurisdictions** with Australia, Macao SAR, Canada, Indonesia and Brunei joining the network in 2025. Through real-time intelligence sharing and coordinated joint operations, FRONTIER+ has been instrumental in dismantling scam syndicates, recovering illicit funds, and disrupting cross-border scam networks.

14. Between February and March 2025, the ASCom **conducted the first Operation FRONTIER+** with Malaysia's National Scam Response Centre and several of Malaysia's government agencies. This led to the freezing of more than 3,400 bank accounts, leading to a recovery of over $2 million and the arrest of over 300 persons.

15. Between May and June 2025, the ASCom **conducted one of the biggest anti-scam operations with the anti-scam units of six overseas law enforcement agencies under FRONTIER+**, namely Hong Kong SAR, Macau SAR, Malaysia, Thailand, the Republic of Korea and the Republic of Maldives. The operation, which involved over 2,780 law enforcement officers, resulted in the freezing of over 32,600 bank accounts, recovery of more than $26.2 million and the arrest of over 1,800 persons.

Engagement

Project A.S.T.R.O. – Leveraging mass distribution of SMSes to alert scam victims

16. To complement enforcement, the ASCom also focused on upstream interventions to identify and alert victims and leveraged technology to strengthen its sense-making capabilities. Through the 'Automation of Scam-fighting Tactics & Reaching Out', also known as Project A.S.T.R.O., the ASCom works with banks such as OCBC, UOB and DBS in automating information-sharing, information-processing and mass distribution of SMS alerts to scam victims. Many of these victims only realised that they had fallen prey to scams after receiving SMS alerts from the Police advising them to immediately cease any further monetary transfers. In the first half of 2025, the ASC has worked with its partnering banks through three joint operations to send out more than 19,800 SMSes to alert more than 14,200 victims. **This proactive victim-centric approach averted over $145 million of potential losses**.

Proactive interventions with potential scam victims

17. The ASCom and the Community Policing Units of the Police Land Divisions regularly conduct joint proactive interventions with potential scam victims. These victims were referred by the financial institutions as they had attempted monetary transfers observed to be suspicious. **In the first half of 2025, 560 such interventions were conducted, averting more than $33.7 million of potential losses**.

Education

18. The SPF has continued its public education efforts to encourage individuals to proactively adopt anti-scam measures, and raise awareness on scam types, including through partnerships with community stakeholders to co-create and amplify anti-scam initiatives.

Encouraging adoption of protective measures and actions

Increased adoption of the ScamShield Suite of anti-scam resources

19. The SPF, in partnership with the National Crime Prevention Council (NCPC) and Open Government Products (OGP), harmonised the different anti-scam resources under the "ScamShield" brand since September 2024 to make scam related channels and resources more accessible to members of the public, and enable them to better protect themselves against scams. The anti-scam resources under the ScamShield Suite are:

i. 24/7 ScamShield Helpline 1799 – Call to check if they are unsure if something is a scam;

ii. ScamShield app – Block scam calls and detect scam SMSes; check and report if a suspicious call, message or website is a scam;

iii. ScamShield website (www.scamshield.gov.sg) – One-stop portal on scams; learn about latest scam trends and protective measures;

iv. ScamShield Alert social channels on WhatsApp and Telegram – Receive latest information on scams and protective actions.

20. **The usage of the anti-scam resources have seen a steady increase since the launch of the ScamShield Suite.**

21. The **ScamShield app** which allows users to check and report if suspicious calls, messages and websites are scams has over 1.34 million downloads, 1.27 million user checks and 599,700 user reports. The **24/7 ScamShield helpline** has received over 128,000 calls and online chats since its launch, and currently receives around 500 to 700 calls daily. Of the calls received, around 80% called to check if something is a scam, with the helpline operators assisting callers to avert scams. The **ScamShield Alert social channels** have over 92,700 subscribers, and the **ScamShield website** has garnered over 2.24 million visitors since its launch.

"I can ACT against Scams" campaign

22. The SPF, supported by the NCPC, will continue to promote the "I can ACT against Scams" campaign. Launched in January 2023, the objective of the campaign

is to encourage people to take protective actions against scams. The campaign promotes three simple anti-scam actions – Add, Check, Tell. From January 2023 to October 2024, the campaign focused on the "Add" part of the framework, to encourage public to adopt protective measures such as the ScamShield app, anti-virus software, Money Lock and International Call Blocking Option.

23. Since November 2024, a new phase of the campaign was launched, which focused on the "**Check**" part of the framework. It encouraged individuals to "Stop and Check" before making monetary transfers and making decisions. This serves as a cognitive break, potentially helping individuals better identify the situation he or she is in and whether a scam was likely present. The campaign also promoted key official resources (e.g. ScamShield Helpline "1799" and ScamShield app) that the public can use to check if something is a scam.

Raising awareness on scam types and latest scam variants

Anti-scam publicity via targeted media campaigns

24. In addition to the timely dissemination of information on the latest scam trends, the SPF has been working on monthly media campaigns to promote the public's awareness of scams with high losses, such as government officials impersonation scams, investment scams and job scams. Anti-scam content was weaved into different mediums, such as short-form advisories, multimedia articles, interactive content, videos, radio interviews etc to reach different population segments.

25. The SPF also worked with partners to proactively develop anti-scam advisories to warn members of the public of potential new scams before they proliferate. For example, in the first half of 2025, SPF worked with the Elections Department Singapore to develop content on a phishing scam variant whereby victims were asked to restore their name in the Register of Electors. More recently in July 2025, SPF also developed anti-scam advisories to warn members of the public about fake SG60 vouchers advertisements on social media and messaging apps, and phishing websites.

Rallying the community to fight against scams

Tapping on the networks of government, community and industry partners to amplify anti-scam messaging

26. The SPF has been engaging government, community and industry partners to help amplify public education on scams, to reach out to different population segments more effectively.

- In engaging the elderly group, the SPF worked with Love-Link Service Society to educate the elderly on scams through monthly luncheons for around 800 participants islandwide. SPF also worked with InTune Music to release a mandarin anti-scam song "Suspect X!", on 16 June 2025 across major digital

music platforms. The song was performed by local artistes 'LimTayPeng' and past contestants of Golden Talentime, and has since been performed at events such as the Papazao 3rd Anniversary walk on 13 July 2025 to over 3,000 participants. The SPF also collaborated with the Singapore Chinese Cultural Centre to produce a Chinese opera troupe-inspired anti-scam video "Don't fall for scams. A.C.T. against scams today!" to engage the vernacular-speaking groups. The SPF also works closely with the Ministry of Digital Development and Information to incorporate anti-scam messages in vernacular languages, such as gov.sg dialect drama "We are number 1".

- The SPF, CSA and NCPC partnered Meta and Eyeyah! on an online interactive website "Is this Legit?". Collaborations were also done with Google and Bamboo Builders via the SG SCAMWISE anti-scam initiative which the public can access.
- The SPF works closely with the Ministry of Manpower and NGOs to educate migrant workers and migrant domestic workers on scam prevention through talks, free courses and collaterals translated into the workers' native languages. These collaterals are also shared with employers and dormitory operators, for them to help reinforce vigilance among workers.

Anti-scam roadshows for the public

27. SPF is also working with partners on roadshows to reach out to members of the public on scams. Members of the public can look forward to such roadshows from the fourth quarter of 2025, which they can attend to learn how to protect themselves from scams through engaging displays and activities.

Exploring games as a tool to facilitate learning about scams

28. Beyond the NCPC #XiamTheScams web-based life simulation game, which engaged over 519,000 players from 24 October 2024 to 22 January 2025, the SPF continues to explore the use of gamification to develop anti-scam centric active learning experiences for the public. For example, the SPF is working with community partners such as KidsPlaySafer and Digi-Up! to incorporate scam related messages into their ground-up games that are developed for the community.

'Cyber Guardians on Watch' interest group of the Community Watch Scheme

29. The 'Cyber Guardians on Watch' was launched during the Police Workplan Seminar in May 2024 as part of an effort to tackle a broad range of cybercrimes. Members of the 'Cyber Guardians on Watch' come from all walks of life and are encouraged to be the SPF's eyes and ears to report any suspicious activity and safeguard our cyberspace. Members receive targeted cybercrime-related information, alerts and advisories from the Police through the Police@SG app. They help to amplify the alert messages by sharing such information with their family and friends. As of 30

June 2025, there were more than 40,000 members in the Cyber Guardians on Watch interest group.

Cyber Crime Prevention Ambassador Programme

30. To strengthen its efforts against cybercrime and scams and galvanise individuals to take a more active role in safeguarding themselves, NCPC launched the Cyber Crime Prevention Ambassador (Cyber CPA) programme in May 2024. This group of volunteers has undergone training and are deployed at roadshows and community events to disseminate cybercrime prevention messages. Since its launch, the Cyber CPAs have reached out to more than 46,000 members of the public across 145 events.

E-commerce Marketplace Transaction Safety Rating

31. The E-commerce Marketplace Transaction Safety Rating (TSR) was launched in May 2022 to raise consumer awareness of the extent to which different e-commerce marketplaces have put in place safety features to protect their users from scams.

32. TikTok Shop has been added in the latest refresh of the TSR in 2025. Shopee, Amazon, Lazada, and TikTok Shop have implemented all the safety features deemed critical by MHA to address e-commerce scams and have notably fewer scam cases than Carousell and Facebook Marketplace. In particular, the number of e-commerce scam cases on Carousell is more than the number of scam cases of the other five platforms combined.

33. MHA encourages all e-commerce marketplaces to put in place the recommended safeguards, specifically user verification against Government-issued documentation and secure payment options. These measures have proven to be effective in combatting scams. MHA will continue to monitor the e-commerce scams situation on Facebook and Carousell and will consider imposing additional measures through the Online Criminal Harms Act (OCHA) if necessary.

Annex G

Whole of Government's Efforts to Fight Scams and Cybercrime

Anti-scam measures by the Monetary Authority of Singapore (MAS)

34. MAS continues to collaborate with other Government agencies and lead the financial industry to strengthen defences against scams.

35. Major retail banks have phased out SMS one-time passwords for authentication of debit or credit card transactions by digital token users and implemented additional verification for provisioning of cards into mobile wallets. These measures have made it more difficult for a scammer to perform fraudulent card transactions or provision a customer's card into his own mobile wallet.

36. The usage of Money Lock continues to grow. As of 30 June 2025, at least 370,000 customers have locked up more than $30 billion of savings. Banks will continue to encourage their customers to use this service to limit potential losses should a customer's digital banking access be compromised.

37. In December 2024, MAS and the IMDA implemented the Shared Responsibility Framework (SRF). The SRF complements anti-scam measures by strengthening the direct accountability of financial institutions and telecommunications providers to consumers for losses incurred from phishing scams. An additional fraud surveillance duty to detect rapid drainage of large sums from customer accounts came into effect under the SRF on 16 June 2025.

38. Major retail banks will progressively introduce cooling-off periods for high-risk activities, such as increasing transaction limits or changing contact details, to provide potential victims an opportunity to re-assess their actions. MAS is also working with banks on a Fast IDentity Online (FIDO)-compliant hardware token that must be inserted into a customer's device to approve higher value internet banking payments and transfers.

39. Overall, these measures will introduce more friction and could impact legitimate transactions. While banks will do their best to minimise the inconvenience and give time for customers to get used to the new measures, there will be a need to prioritise security over convenience in the ongoing fight against scams.

40. Cryptocurrencies are especially susceptible to scams. Investors should be wary of websites and chat groups promoting cryptocurrency with promises of high returns or endorsements from high-profile personalities. These may well be fraudulent. MAS will continue to develop public education initiatives to strengthen awareness of newer scam typologies, including those relating to cryptocurrency.

Anti-scam measures by the Cyber Security Agency of Singapore (CSA)

41. In February 2024, CSA partnered Google on a pilot for Enhanced Fraud Protection (EFP) within Google Play Protect in Singapore. This feature automatically blocks the installation of potentially malicious apps that use sensitive runtime permissions. As of June 2025, the EFP feature has successfully blocked 2.49 million installation attempts of potentially malicious applications across 553,000 devices. This prevented more than 40,000 unique apps from potentially being misused for financial fraud and scams. This feature is now being rolled out in other countries by Google, protecting citizens beyond Singapore.

42. From April to June 2025, the SPF, HKPF, and Royal Malaysia Police (RMP) conducted a joint operation that successfully disrupted a criminal syndicate operating Voice over Internet Protocol (VoIP) GSM gateway devices used to perpetrate scam calls. CSA provided critical technical expertise in multiple aspects of the operation. This included conducting research and tests with the GSM gateway devices to analyse network communication protocols.

43. CSA's technical analysis and forensic capabilities provided vital leads to overseas syndicate and other GSM gateways. This helped facilitate operations with partners to trace devices across Singapore, Malaysia and Hong Kong. 11 suspects were arrested across the three jurisdictions, and more than 200 GSM gateway devices were seized.

44. CSA will launch its sixth National Cybersecurity Campaign on 13 September 2025 at Waterway Point. Building on insights from the CSA Cybersecurity Public Awareness Survey 2024, the campaign will highlight the importance of cybersecurity practices, i.e. installing security apps, enabling two-factor authentication (2FA) and setting strong passphrases, as well as updating software regularly. The campaign will also comprise roadshows, corporate partnerships, talks, with posters and videos running on various online and out-of-home platforms.

45. CSA partners the Ministry of Education to develop resources for educators and students on online dangers and steps to protect themselves. A mobile Be Cyber Safe Pop-Up, comprising an interactive vending machine and digital information panels, as well as drama skits and school talks have been conducted to support schools in cybersecurity education. Since January 2024, the Pop-Up has travelled to over 150 schools and community events, while the drama skits have been seen by over 138,400 primary to junior college students.

46. CSA also drives efforts to help seniors stay safe online through various partnerships. CSA has been working with IMDA's SG Digital Office to reach out to seniors through its Digital Ambassadors. CSA also partnered with IMDA and DBS Foundation to co-develop a bite-sized beginner's guide to Generative AI for seniors to

understand both its creative uses and associated risks, along with advice on how to use new technologies safely.

Anti-scam measures by the Government Technology Agency Singapore (GovTech Singapore)

47. GovTech Singapore continues to collaborate with SPF and HTX to enhance the Scam Analytics and Tactical Intervention System (SATIS) suite of products. SATIS leverages artificial intelligence and machine learning to swiftly triage, assess and disrupt scam-related websites. A similar system called SATIS+ disrupts other scam enablers such as online monikers and payment channels, with planned improvements to disrupt mobile numbers.

Anti-scam measures by the Open Government Products (OGP)

Single SMS Sender ID, 'gov.sg'

48. Since 1 July 2024, the Singapore Government has implemented a single SMS Sender ID, 'gov.sg', for all government agencies. This replaces most individual government agency Sender IDs. The change aims to help the public easily identify genuine government SMS communications and protect against government officials impersonation scams, with 0 scam SMSes sent from gov.sg ID. To date, 181 million SMSes have been sent out, and 93% of the public recognise the gov.sg SMS channel. gov.sg has also grown to serve 66,140 agency users, attaining an 84.3% positive satisfaction score.

ScamShield app

49. In August 2024, OGP enhanced the ScamShield app to move from passive to active protection, addressing emerging scam variants more effectively. The enhanced app enables users to check suspicious calls, messages and websites on third-party platforms such as WhatsApp and Telegram. Reporting has also been streamlined, allowing more crowdsourced data to strengthen scam detection and intelligence. These improvements optimise the performance of ScamShield's AI classifier, ensuring scam calls and SMSes are detected with greater accuracy.

50. Since then, there has been a 42% growth in the app user base from 944,000 to 1.34 million users currently. More than 327,000 activated users have used the "Check for Scams" or "Report a Scam" feature at least once and have rated the app an average of 4.6/5 for in-app satisfaction.

'Unpacked' mobile immersive scam simulation

51. 'Unpacked' is an immersive, mobile-first simulation that lets users experience a scam firsthand to better understand how it unfolds. Built during OGP's Hack for Public Good 2025, 'Unpacked' walks users through a realistic government officials impersonation scam, beginning with a phone call from someone claiming to be the police. As the story unfolds, users are asked to make decisions under pressure, leading up to a simulated bank transfer. At the end, a reflective debrief explains how scammers build trust and create urgency, while sharing practical tips to stay safe. Since February 2025, 'Unpacked' has hosted more than 9,920 unique visitors.

Anti-scam measures by the Infocomm Media Development Authority (IMDA)

52. IMDA continues to partner the SPF and telecommunications companies in Singapore to implement measures that strengthen our defence against scam calls and SMSes, and this has seen results. [3]

53. Through these efforts, close to 100 million potential scam calls and 12 million potential scam SMS messages were successfully blocked in the first half of 2025.

Features to block international calls and SMSes

54. Today, all telecommunications companies in Singapore offer the features to block all incoming international calls and SMSes on mobile and residential fixed lines. To date, over 800,000 subscribers have activated the feature to block overseas calls and over 200,000 subscribers have activated the feature to block overseas SMSes. Subscribers are encouraged to activate the features to prevent the incidence of receiving scam calls and SMSes from overseas numbers if they do not expect to get any overseas calls or SMSes in the first place. Subscribers can also check in with their respective telecommunications companies for more information on how to activate the features.

Detecting suspicious numbers

55. To further safeguard the public against scam calls, IMDA has been working with telecommunications companies to detect and act against the suspected misuse of local mobile numbers based on suspicious traits.

Anti-scam measures by the Central Provident Fund Board (CPFB)

56. In April 2025, as part of nationwide efforts in tackling government officials impersonation scam, the CPFB has consolidated all outbound calls into a single number. **All calls from the CPFB will only be made from 6227 1188**. This number is listed on CPFB's website, whitelisted in the ScamShield application, and publicised

[3] More information on IMDA's anti-scam measures can be found at https://www.imda.gov.sg/how-we-can-help/anti-scam-measures.

on CPFB's advisories and social media platforms to allow members to easily verify the authenticity of calls from the CPFB.[4]

57. For missed calls from CPFB, members would receive a gov.sg SMS or email notification from an address ending with @cpf.gov.sg or @e.cpf.gov.sg with callback details.

58. This consolidation to a single number is in addition to CPFB's existing suite of anti-scam measures, which includes the online Daily Withdrawal Limit (DWL), the CPF Withdrawal Lock, enhanced authentication and a 12-hour cooling period for increases to the DWL, and updates to registered bank account information or contact details.

59. The public continues to play a crucial role in combating scams. CPFB actively engages members through various touchpoints, particularly those who are eligible to make CPF withdrawals from age 55, to remind them to stay vigilant and to encourage them to activate the CPF Withdrawal Lock to disable online withdrawals if they have no intention to withdraw their CPF savings anytime soon.

[4] More information on CPFB's anti-scam measures can be found at www.cpf.gov.sg/antiscamtips.