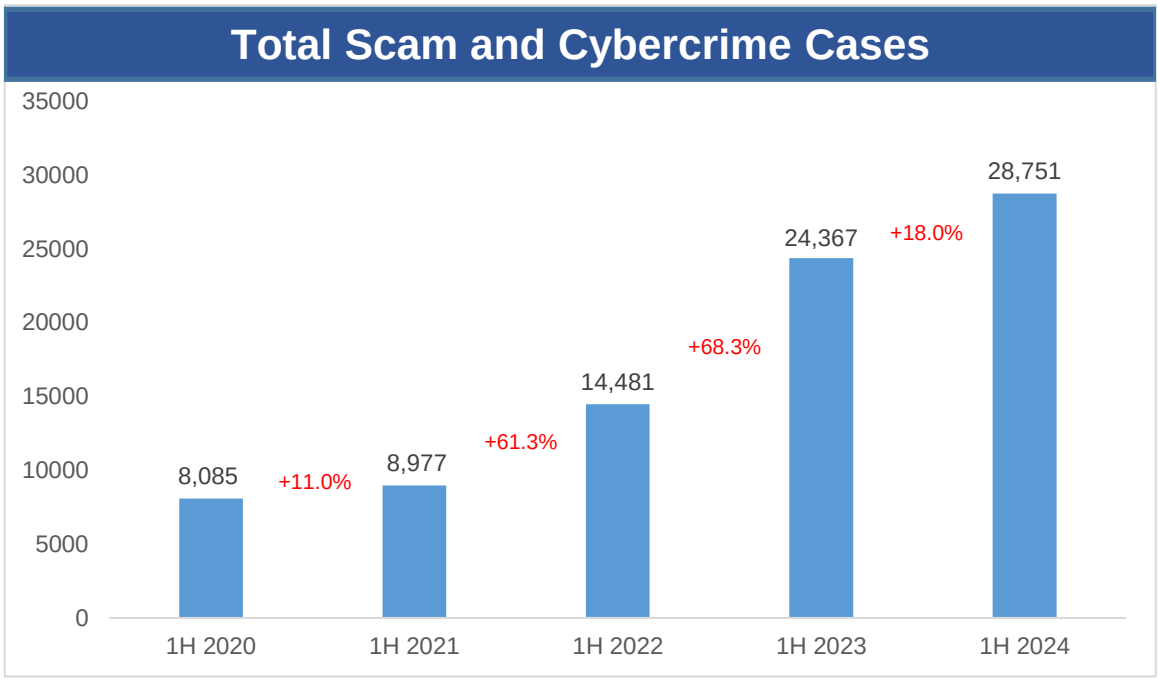
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

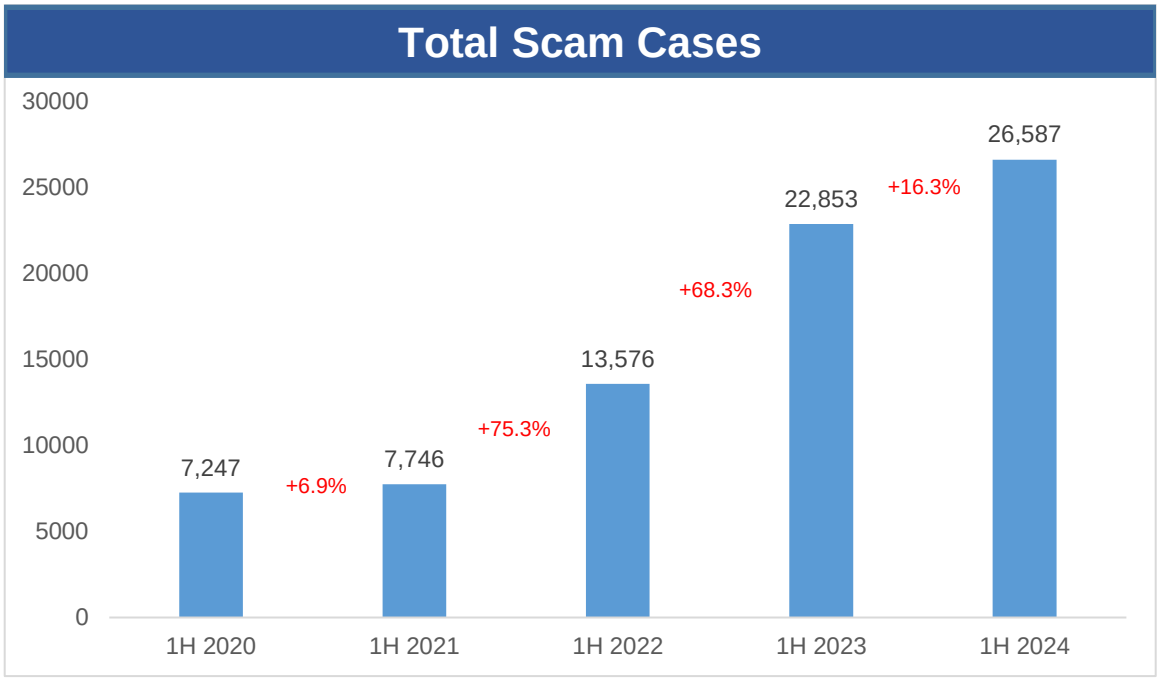
Mid-Year Scams and Cybercrime Brief 2024

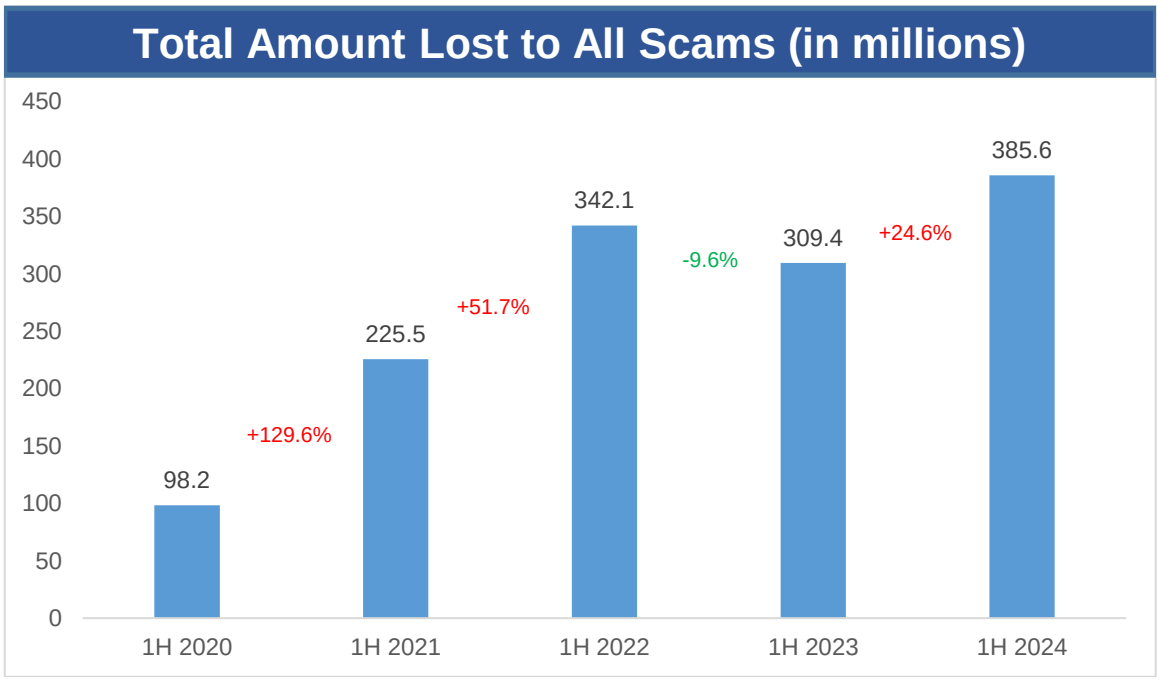
Overall Scams and Cybercrime Situation for January to June 2024

Scams and cybercrime continue to be a key concern. From January to June 2024, the number of scam and cybercrime cases increased by 18.0% to 28,751 cases, compared to 24,367 cases in the same period in 2023.



2. Scams accounted for 92.5% of these 28,751 cases. The total number of scam cases increased by 16.3% to 26,587 cases in the first half of 2024, from 22,853 cases in the same period last year. The total amount lost increased by 24.6% to at least $385.6 million in the first half of 2024, from at least $309.4 million in the same period last year.





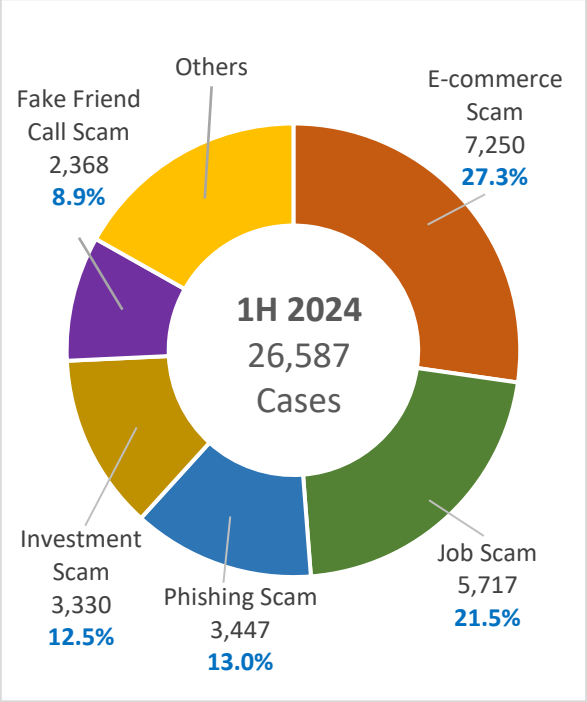
3. Overall, the average amount lost per scam case for all reported scam cases has increased, by about 7.1% to $14,503 in the first half of 2024, from $13,541 in the first half of 2023. 59.8% of scams cases in first half of 2024 have losses less than or equal to $2,000.

4. **86.0% of total reported scams involved mostly self-effected transfers** which may be a result of deception and social engineering involving an array of complex scam methods. In most of these cases, scammers did not gain direct control of victims' accounts, but manipulated victims into directly performing the monetary transactions.

Top Scam and Cybercrime Concerns

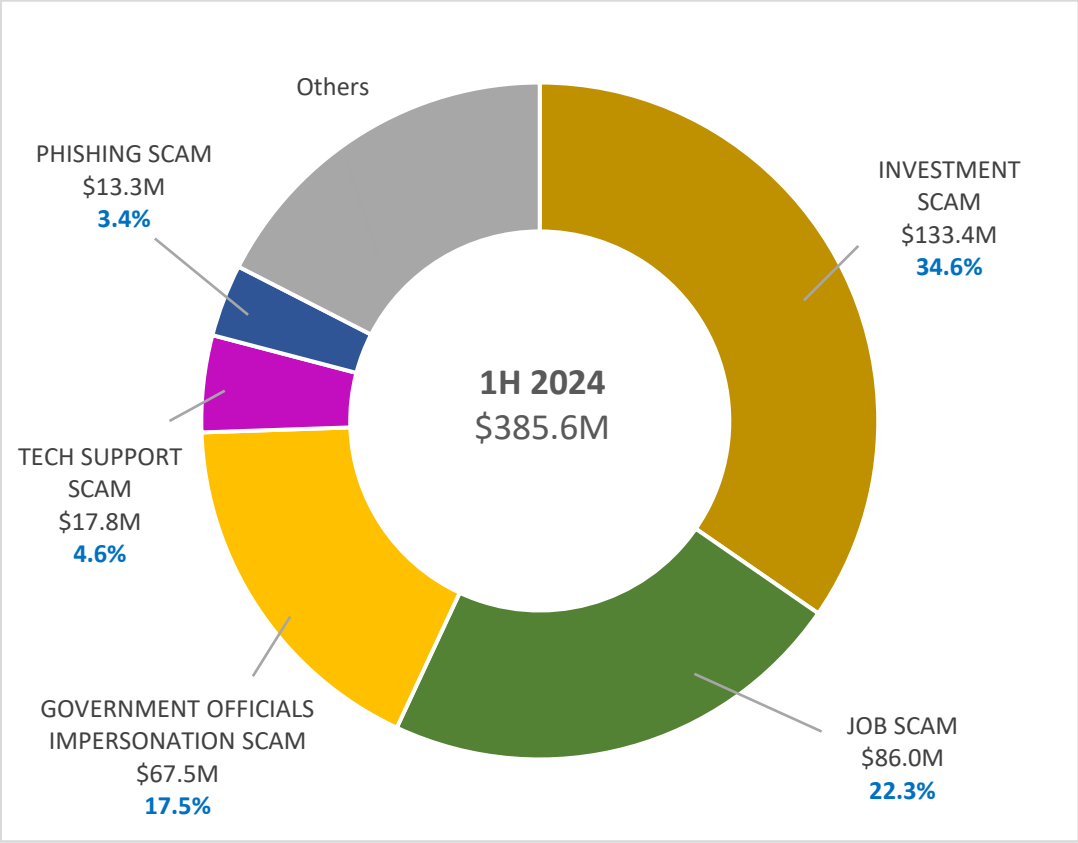
5. **In terms of the number of scam cases, e-commerce scams, job scams and phishing scams were the top three scam types in the first half of 2024.**

Breakdown of scam types by number of cases



6. In terms of the total amount lost, investment scams, job scams and government officials impersonation scams were the top three scam types in the first half of 2024.

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



7. Among the top ten scam types in the first half of 2024 (see **Annex**), **government officials impersonation scams had the highest average losses at about $116,534 per case, followed by investment scams at about $40,080 per case**. These two scam types typically involve deception and social engineering conducted over a period of time, using an array of complex scam methods.

8. **Fake friend call scam cases decreased by 38.2% to 2,368 cases in the first half of 2024,** from 3,832 cases in the same period last year, and **total amount lost also decreased by 37.2% to about $8.1 million**, from at least $12.9 million in the same period last year. **Malware-enabled scam cases also decreased by 86.2% to 95 cases in the first half of 2024**, from 687 cases in the same period last year, and **total amount lost decreased by 96.8% to about $295,000**, from at least $9.1 million in the same period last year.

a) E-commerce scams

i. E-commerce scams recorded the highest number of reported cases among all scam types in the first half of 2024. There were 7,250 cases reported and the total amount lost from e-commerce scams was at least $8.6 million.

ii. 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

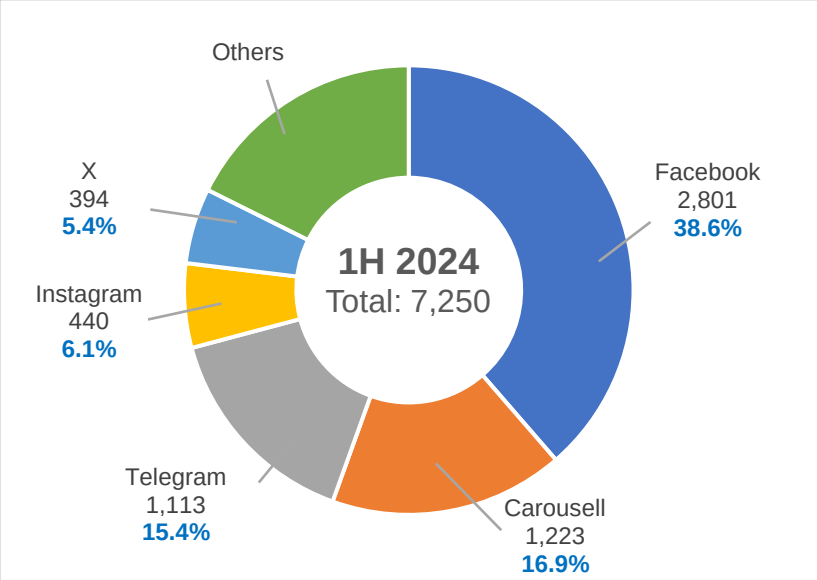
some cases, the victims could also be sellers who did not receive payment after delivering the goods or services to scammers pretending to be buyers. The scammers sometimes provided victims with fake screenshots as “proof of payment”.

iii. Concert tickets were the top item involved in e-commerce scams. Victims typically came across concert ticket listings on social media or online marketplaces, 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.

iv. Other items commonly featured in e-commerce scam cases were rental of residences and electronic goods.

v. The majority of e-commerce scam victims were aged 30 to 49, accounting for 44.3% of victims for this scam type. The most common platforms on which e-commerce scams were conducted included Facebook, Carousell and Telegram. The breakdown of e-commerce scams on the various platforms are as follows:

Top five digital platforms used in e-commerce scams in first half of 2024



b) Job scams

i. Job scams recorded the second highest number of reported cases among all scam types in the first half of 2024. There were 5,717 cases reported and the total amount lost was at least $86.0 million.

ii. Job scams typically involve victims being offered online jobs that could be performed from home. Victims would 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 also chance upon “job opportunities” through social media platforms like Instagram or Facebook or through their own internet searches. Victims would be asked to perform simple tasks for a commission, such as liking or following social media posts or accounts, booking or reviewing hotels/restaurants/airlines, making advance purchases, completing surveys, “boosting” value of cryptocurrencies, “boosting” ratings of product listings for online merchants, or “rating” mobile apps to improve their rankings on app stores. Another “job” offered to victims entails transfer of funds to bank accounts provided by the scammers, for a small commission. The scammers would subsequently request higher amount of funds to be transferred, for purportedly higher earnings. 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 from the bank accounts, or when the scammers could no longer be contacted.

iii. 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.

iv. The majority of job scam victims were aged 30 to 49, making up 44.0% of victims for this scam type. The most common platforms which scammers used to contact job scam victims were WhatsApp and Telegram.

c) <u>Phishing scams</u>

i. There were 3,447 phishing scam cases reported in the first half of 2024, with total amount lost of at least $13.3 million.

ii. 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 usernames, passwords, banking credentials and/or debit or credit card information by 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.

iii. Some phishing scam variants include the following actions by scammers:

- Posing as interested buyers through marketplace platforms – Scammers would pose as potential buyers and approach victims by expressing interest in items listed for sale on online marketplace platforms such as Carousell and Facebook Marketplace. Victims would receive malicious URL links or QR codes via email or in-app messaging under the pretext of receiving payment for items or to pay for courier services to facilitate the delivery of the items. Upon clicking the malicious links, victims were led to spoofed bank or delivery company websites where victims were prompted to key in their banking credentials, debit/credit card details and One-Time-Passwords (OTPs).

- Impersonation of government officials through calls – Victims would receive unsolicited phone or in-app calls allegedly from government officials such as the Singapore Police Force (SPF), Immigration & Checkpoints Authority and the Ministry of Manpower (MOM). 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, OTPs and/or personal details.

- Impersonation of banks through spoofed SMSes – Victims would receive unsolicited SMSes from both overseas and local numbers, or short codes impersonating banks. The spoofed SMSes "warned" victims of possible unauthorised transactions in their bank or credit card accounts, and instructed them to click on embedded links for verification or to stop the transactions. Victims were then directed to spoofed banking websites after clicking on the embedded links and were misled into providing their banking credentials, debit/credit card details or OTPs that allowed scammers to perform unauthorised transactions.

iv. In these variants, victims would discover that they had been scammed when they found unauthorised transactions made from their bank accounts or debit/credit cards.

v. The majority of phishing scam victims were aged 30 to 49, comprising 44.4% of victims for this scam type. Carousell, Facebook and SMS were the most common channels used by phishing scammers to contact potential victims.

d) Investment scams

i. There were 3,330 investment scam cases reported in the first half of 2024, resulting in a total loss of at least $133.4 million.

ii. Victims of investment scams usually came across “investment opportunities” through their own internet searches or via recommendations from online friends. Some victims also received unsolicited messages from scammers offering “investment opportunities”. Once they were duped or had been enticed by the false testimonies, they transferred funds to specified bank accounts or cryptocurrency wallets or made payments via their bank cards for their “investments”. In some cases, 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. The victims might also be deceived by the scammers’ use of “investment” websites or apps to display their “profits” and be convinced to invest more monies. After larger amounts of monies or cryptocurrencies were transferred to the scammers for their “investment”, they would experience difficulties withdrawing their earnings from their “investments” and only then realise that they had been scammed.

iii. In another approach, scammers would add victims into chatgroups or channels via messaging platforms such as WhatsApp and Telegram, purportedly for “investment opportunities”. In these chatgroups or channels, the victims were presented with multiple claims from other members who had “profited” from their investments, convincing the victims of the authenticity of the investments. Tempted by the promised returns, the victims would contact the scammers. They would then share personal information with the scammers to “set up accounts” and transfer funds for “investment”. Before receiving the earnings from their “investments”, the victims were instructed by the scammers to transfer monies for various “fees” incurred for the “investment”. The victims would realise that they had been scammed when they were unable to withdraw their “profits” despite paying the incurred “fees” for the “investments”.

iv. The majority of investment scam victims were aged 30 to 49, making up 44.7% of victims for this scam type. Telegram, Facebook and WhatsApp were the most common platforms used by investment scammers to contact potential victims.

e) Government officials impersonation scams

i. There were 580 government officials impersonation scam cases reported in the first half of 2024, with a total amount loss of at least

$67.5 million. The number of government officials impersonation scam cases increased by 58.0% from 367 cases reported in the same period last year. The total amount lost from government officials impersonation scams also increased by 67.1%, from at least $40.4 million in the same period last year.

ii. Government officials impersonation scams typically involve scammers impersonating local government officers [e.g. SPF, Immigration & Checkpoints Authority (ICA), Monetary Authority of Singapore (MAS)], bank staff (e.g. DBS, UOB) or China government officials (e.g. China Police). The two variants include the following actions by scammers:

- Impersonation of bank staff and local government officials through calls – Victims would receive unsolicited calls from scammers impersonating bank staff (e.g. DBS, UOB) seeking verification on banking transactions allegedly conducted by victims. When victims deny making such transactions or possessing such bank cards, the first scammer would transfer the call to a second scammer claiming to be a government official (e.g. SPF, MAS). This second scammer would accuse victims of being involved in criminal activities (e.g. money laundering). In some cases, victims were transferred to a third scammer for "further investigations". Under various pretexts (e.g. investigation, to verify or safekeep funds), scammers would instruct victims to transfer money to bank accounts supposedly designated by the SPF, MAS or other authorities.

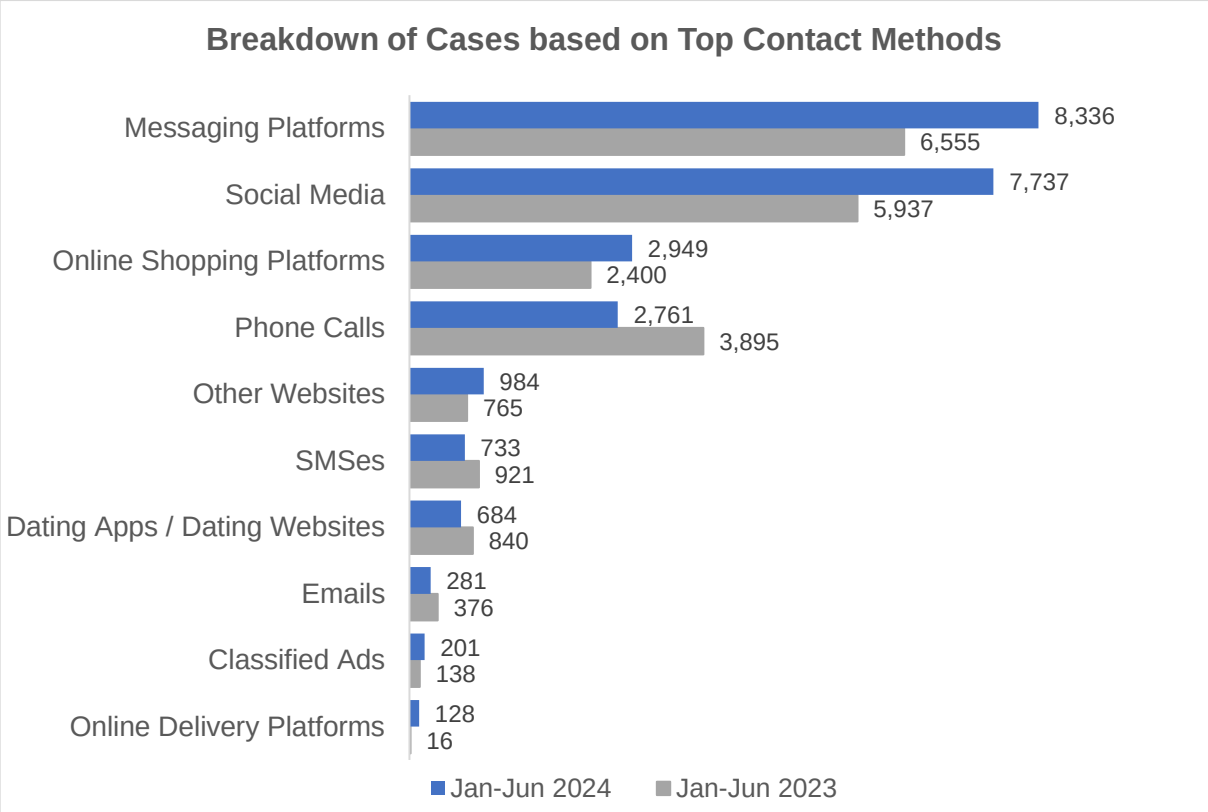
- Impersonation of China government officials (e.g. China Police) and bank staff/local government officials through calls – Victims typically received unsolicited calls from scammers impersonating government officials (e.g. ICA, Ministry of Health) or bank staff (e.g. DBS), who would allege that victims had applied for credit cards, bank accounts or phone numbers that were eventually involved in criminal activities. In some case, scammers alleged that victims were involved in spreading false rumours/ information, had parcels under their names containing prohibited good, or had made illegal purchases. When victims denied being involved, the first scammer would transfer the call to a second scammer claiming to be a China government official (e.g. China Police), who would accuse victims of being involved in criminal activities (e.g. money laundering). Under various pretexts (e.g. investigation, to verify or safekeep funds, bail payment), scammers would instruct victims to transfer money to bank accounts supposedly designated by China authorities.

iii. The majority of government officials impersonation scam victims were aged 65 and above, comprising 28.9% 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.

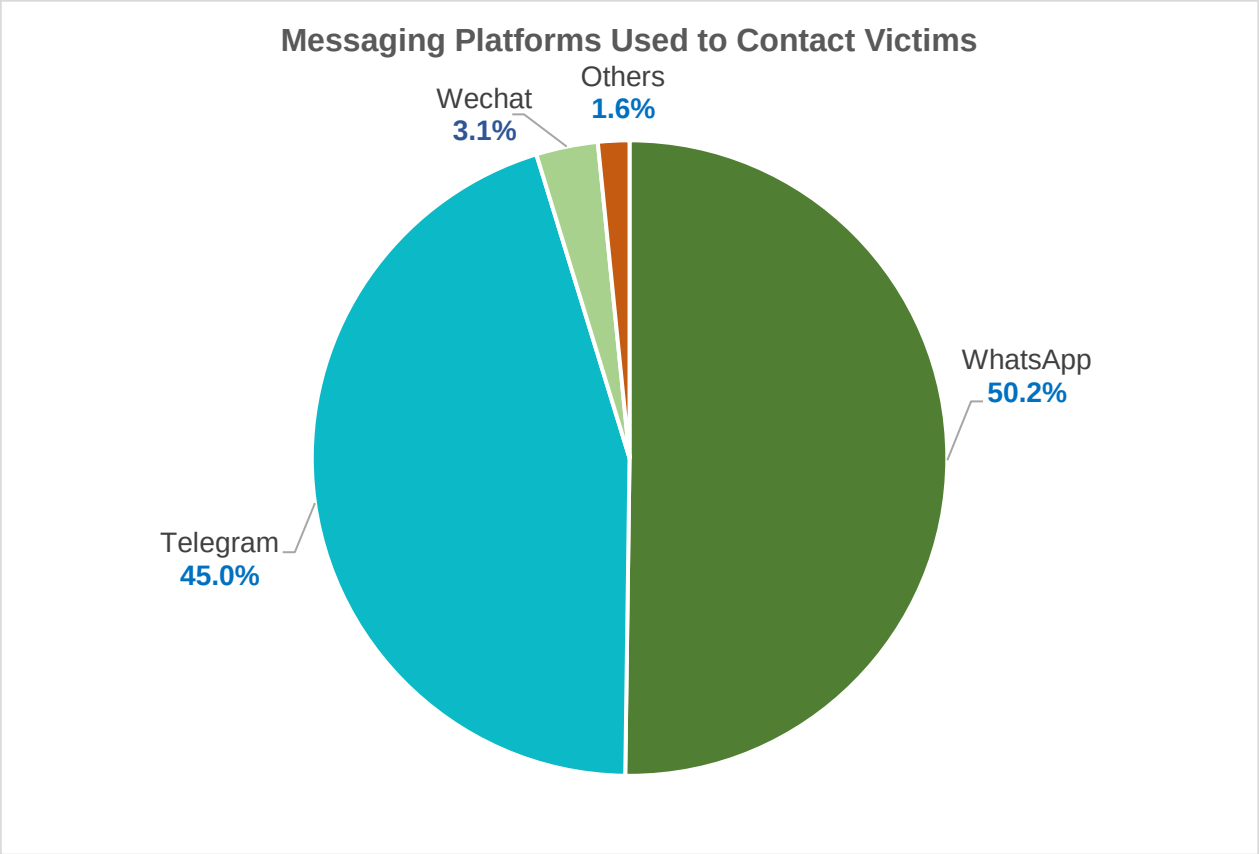
Top Contact Methods

9. Scammers commonly reach out to victims through messaging platforms, social media, online shopping platforms, phone calls and other websites. These methods constitute the top five contact methods used by scammers.

10. Three products from Meta – Facebook, WhatsApp and Instagram – remain particularly concerning, consistently being over-represented among the platforms exploited by scammers to contact potential victims and conduct their scams. In addition, there was a spike in scam cases involving Telegram in the first half of 2024.

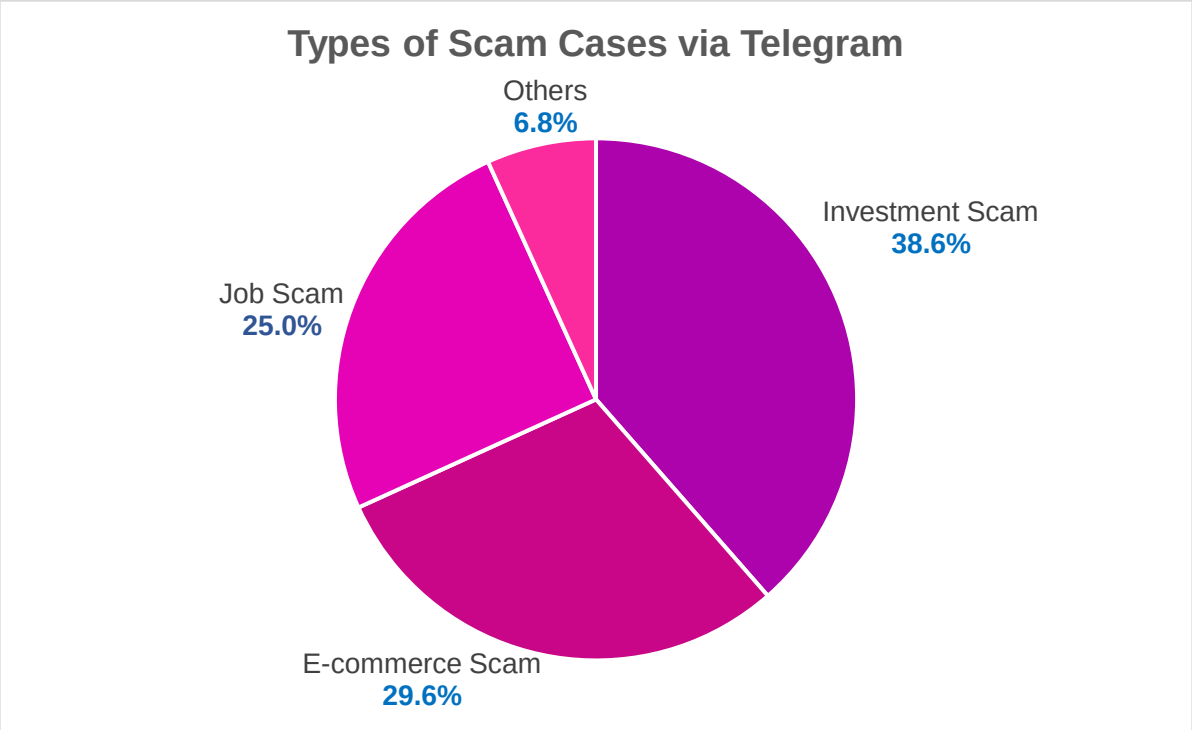


11. In the first half of 2024, the number of scam cases where scammers contacted victims via messaging platforms increased to 8,336 from 6,555 in the same period last year. Approximately 50.2% of the cases were conducted via WhatsApp, and 45.0% via Telegram.

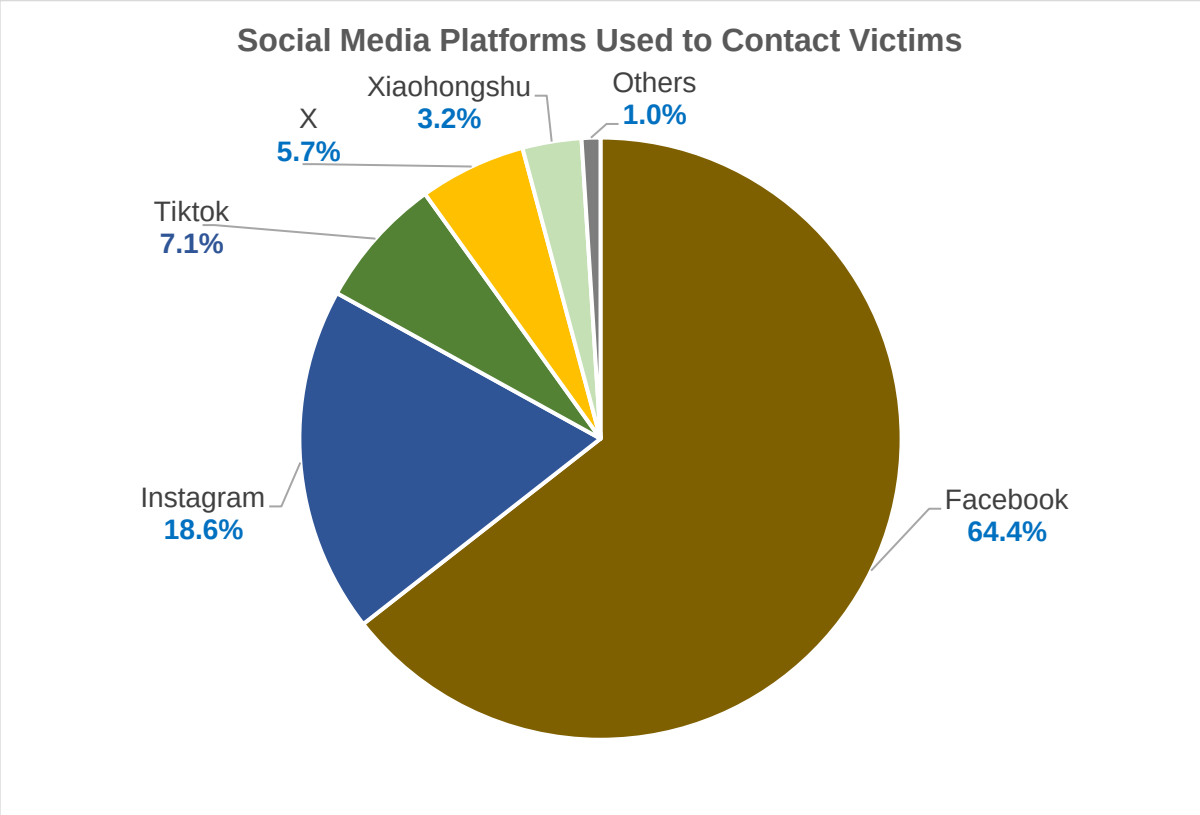


12. Among the scam cases where scammers contacted victims via WhatsApp, 56.8% were job scams, 10.8% were phishing scams and 10.6% were fake friend call scams.

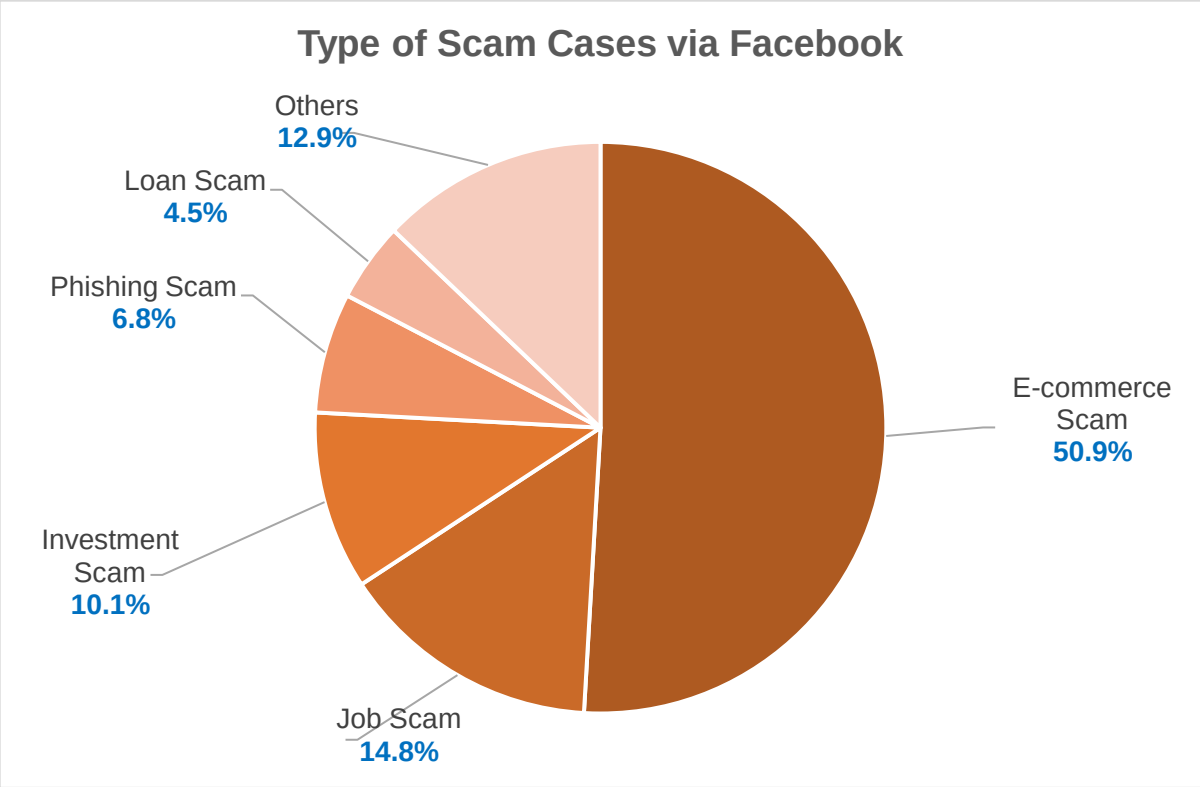
13. **The number of scam cases perpetrated on Telegram saw an increase of about 137.5% in the first half of 2024, from the same period in 2023.** Among the scam cases where scammers contacted victims via Telegram, 38.6% were investment scams, 29.6% were e-commerce scams and 25.0% were job scams.



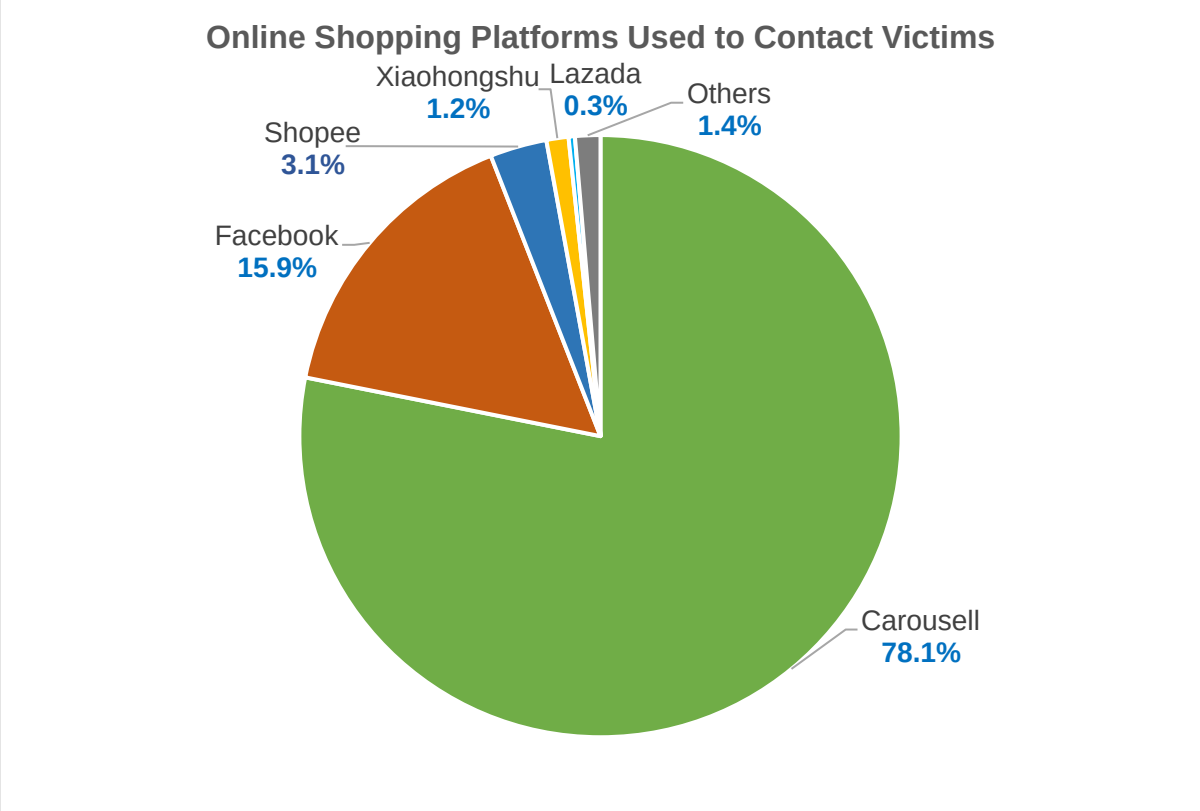
14. The number of scam cases where scammers contacted victims via social media increased to 7,737 in the first half of 2024, from 5,937 in the same period last year, with about 64.4% on Facebook and 18.6% on Instagram.



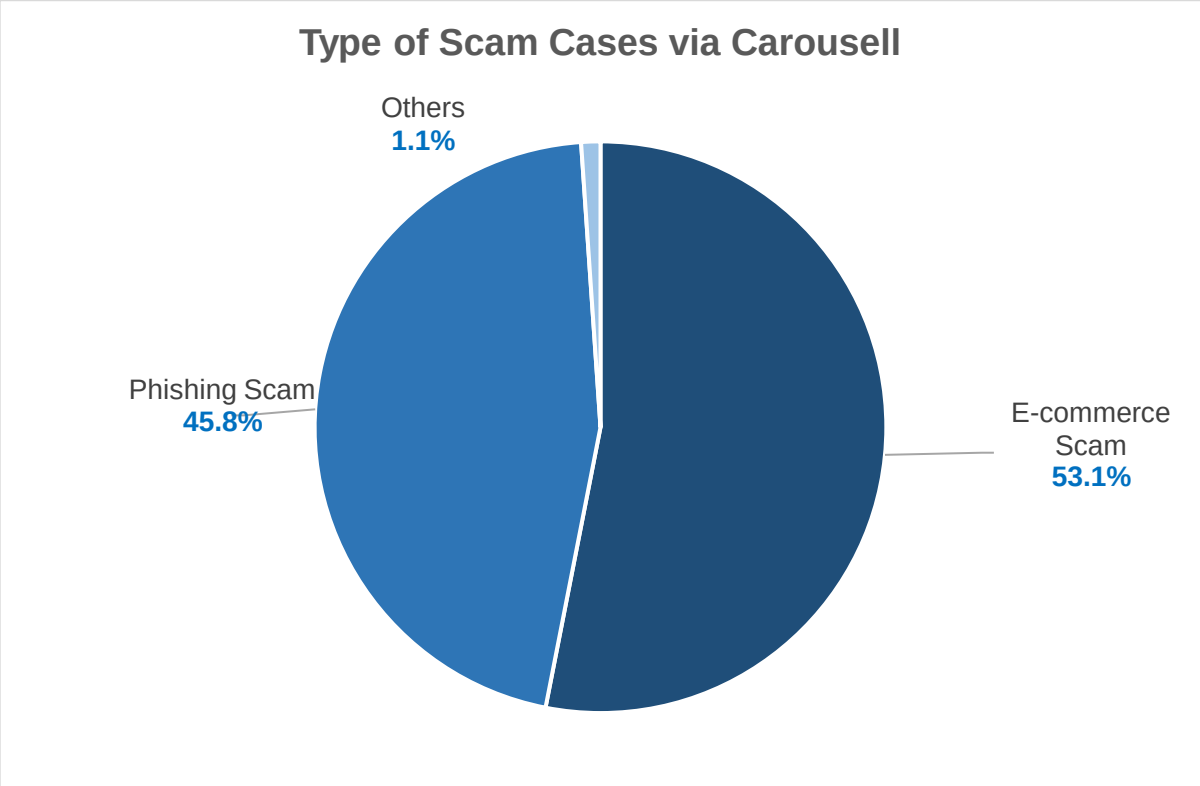
15. Among the scam cases where scammers contacted victims via Facebook, 50.9% were e-commerce scams, 14.8% were job scams, and 10.1% were investment scams.



16. Online shopping platforms is a contact method of concern. The number of scam cases perpetrated via online shopping platforms increased to 2,949 in the first half of 2024, from 2,400 in the same period last year. 78.1% of these cases occurred on Carousell and 15.9% on Facebook.



17. Among the scam cases which victims encountered scammers via Carousell, 53.1% were e-commerce scams and 45.8% were phishing scams.



Scam Victim Profile

18. **74.2% of scam victims were youths, young adults and adults aged below 50 in the first half of 2024. However, the average amount lost per elderly victim is the highest.** The breakdown of scam victims by age group is as follows:

a) Youths, aged 19 and below, made up 7.2% of the scam victims. 44.2% fell prey to e-commerce scams, while 23.1% fell prey to job scams and 12.0% fell prey to phishing scams. Scammers tend to contact youths via Telegram, Carousell and WhatsApp.

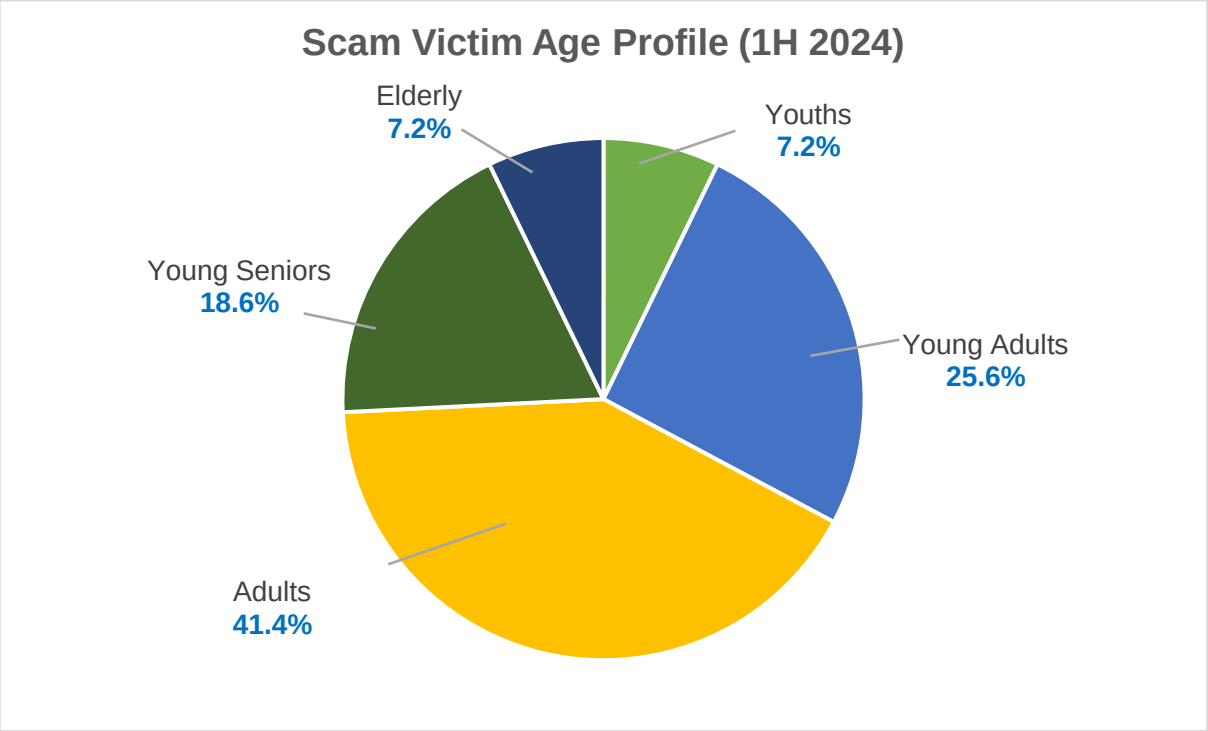
b) Young adults, aged 20 to 29, made up 25.6% of scam victims. 37.1% fell prey to e-commerce scams, while 25.8% fell prey to job scams and 10.8% fell prey to phishing scams. Scammers tend to contact young adults via Telegram, WhatsApp and Facebook.

c) Adults, aged 30 to 49, made up 41.4% of scam victims. 29.9% fell prey to e-commerce scams, while 22.6% fell prey to job scams and 14.1% fell prey to phishing scams. Scammers tend to contact this victim group via Facebook, WhatsApp and Telegram.

d) Young seniors, aged 50 to 64, made up 18.6% of scam victims. 18.9% fell prey to investment scams, while 17.8% fell prey to fake friend call scams and 16.9%

fell prey to job scams. Scammers tend to contact this victim group via Facebook, phone calls and WhatsApp.

e) The elderly, aged 65 and above, made up 7.2% of scam victims. 24.4% of victims fell prey to fake friend call scams, while 19.5% fell prey to investment scams and 14.6% fell prey to phishing scams. Scammers tend to reach out to the elderly via phone calls, WhatsApp and Facebook. **While the elderly made up one of the smallest age group of scam victims, the average amount lost per elderly victim is the highest when compared to victims of the other age groups.** This is a concern as the elderly may potentially lose their entire life savings to scams and are unlikely to recover financially.



Police's Efforts to Fight Scams and Cybercrimes

Enforcement

Maintaining strong public-private partnership

19. The Anti-Scam Command (ASCom) has expanded its partnerships to more than 110 institutions, including financial institutions, card security groups, fintech companies, cryptocurrency houses, remittance service providers, and overseas law enforcement agencies from countries such as Hong Kong, Malaysia and Australia to facilitate the swift freezing of accounts and recovery of funds to mitigate victim losses. This is achieved through establishing point-of contact and direct communication channels with these partners. The ASCom has further strengthened the close working relationships with them, leading to the co-location of staff from six banks and Government Technology Agency (GovTech) within the ASCom. In the first half of

2024, the ASCom froze more than 10,300 bank accounts based on reports referred to the Anti-Scam Centre (ASC) and recovered more than $54 million.

Collaboration with e-commerce platforms to take down scam-related online monikers and advertisements

20. The co-location initiative was expanded to include the co-location of Carousell and Shopee staff within the ASCom. This initiative was instrumental in supporting the ASCom in its swift intervention in scam cases on these platforms. In the first half of 2024, ASCom worked with Carousell, Shopee and other online platforms' staff to identify and take down 2,700 scam-tainted online monikers and suspicious advertisements. We encourage more online platforms, including social media platforms and e-commerce platforms, to work with the SPF and co-locate their staff at the ASCom, so as to boost our collective efforts to combat scams.

Collaboration with local telecommunication companies to terminate phone lines related to scams

21. The ASC works closely with other stakeholders such as local telecommunication companies and e-commerce platforms to act against conduits used for scams. In the first half of 2024, more than 10,300 mobile lines and more than 14,800 WhatsApp lines which were believed to be used in scams, were submitted for termination.

Other law enforcement interventions and operations

Enforcement operations targeting local scammers and money mules

22. In the first half of 2024, the ASCom, together with the Scam Strike Teams in the seven Police Land Divisions, conducted 13 island-wide anti-scam enforcement operations, leading to the investigation of more than 4,000 money mules and scammers. Police have also stepped up our enforcement with more than 300 money mules charged in Court.

Upstream anti-scam measures to combat malware-enabled scams

23. Malware-enabled scams recorded a decrease of 86.2% in number of cases, with a 96.8% decrease in losses in the first half 2024, compared to the same period in 2023. This can be attributed to MAS' and SPF's collaboration with the banks to implement anti-malware measures for banking apps. The banking apps would restrict users' access if they detected sideloaded apps with accessibility granted or screen-sharing. Customers will then receive a pop-up message to uninstall the said apps before they can login to the banking apps. In February 2024, the Cyber Security Agency (CSA) worked with Google to block sideloading of potentially malicious Android apps. To tackle the scam scourge, Police conducted intensive enforcement operations, arresting more than 140 subjects involved in malware-enabled scams and charged over 30 of them between June and October 2023.

Collaboration with GovTech and HTX (Home Team Science and Technology Agency) to detect and disrupt scam-related websites

24. Scam Analytics and Tactical Intervention System (SATIS) was developed in collaboration with GovTech and HTX. SATIS is a customised dashboard that will leverage artificial intelligence and machine learning to triage, assess and disrupt scam websites swiftly. With SATIS, SPF worked with local Internet Service Providers to identify and disrupt over 18,000 scam-related websites in the first half of 2024. To stay ahead of scammers, the SPF will continue working with GovTech and HTX to enhance and expand the capabilities of SATIS.

Suspension of bank accounts of ex-work permit holders who have left Singapore

25. As part of the Government's efforts to tackle scams and money laundering, the SPF, MOM and the MAS are working with the banks progressively to suspend the bank accounts of ex-work permit holders who have left Singapore (e.g. those whose work pass has been cancelled or has expired, and do not have any other valid pass to work or reside in Singapore) to prevent their accounts from being misused by criminal syndicates.

26. For instance, in June 2021, the Police stopped two male subjects during a police roadblock and found the subjects in possession of a large number of bank cards and handphones, and a large amount of cash. Further investigations revealed that about half of the bank cards seized belonged to migrant workers. About one-third of those bank accounts belonged to migrant workers and were used for money laundering after the account holders left Singapore. In total, the bank accounts belonging to migrant workers who had left Singapore were used to receive more than $900,000 in criminal proceeds.

27. All work permit holders whose employment in Singapore has ended are therefore advised to close their bank accounts and transfer or remit the money to their accounts in their home country before leaving Singapore. Work permit holders who require assistance in transferring or remitting money after their bank accounts have been suspended should approach their banks for advice.

Collaboration with foreign law enforcement agencies

28. While most online scams are perpetrated by scammers based outside of Singapore and such cases are difficult to investigate and prosecute, SPF continues to work closely with foreign counterparts and partners such as the Royal Malaysia Police and INTERPOL by exchanging information and conducting joint investigations and operations against transnational scams.

Takedown of scam syndicates through collaboration with overseas law enforcement agencies

29. In the first half of 2024, the close collaboration between SPF and overseas law enforcement agencies resulted in the successful takedown of nine transnational scam syndicates comprising three fake friend call syndicates, four suspected money laundering cells, one phishing scam syndicate and one investment scam syndicate. More than 100 persons based overseas who were responsible for more than 320 transnational scam cases, were arrested.

30. Fake friend call scams recorded a decrease of 38.2% in number of cases, with a 37.2% decrease in losses in the first half of 2024, compared to the same period in 2023. This can be attributed to the collaboration between the SPF and the Royal Malaysia Police to dismantle three fake friend call scam syndicates operating from Johor Bahru, Malaysia, leading to the arrest of 19 overseas syndicate members. Between late December 2023 and early January 2024, three Malaysians were convicted and were sentenced to between 30 and 42 months' imprisonment for their involvement in fake friend call scams. In a separate operation in January 2024, the SPF successfully extradited five syndicate members to Singapore and charged them in court. The arrests and convictions of these syndicate members helped deter other like-minded criminals.

Participation in internationally coordinated scam operations

31. SPF also participates in internationally coordinated operations against scams. In the first half of 2024 from 20 March to 20 May 2024, SPF participated in the INTERPOL's Operation First Light, which involved more than 70 countries. During the operation, more than 1,100 persons were investigated and over 3,500 bank accounts were frozen in Singapore, leading to the recovery of more than $16.7 million. Over $203,000 of virtual assets were also blocked by SPF.

Engagement

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

32. 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. Through three joint operations in the first half of 2024, more than 46,400 SMSes were sent to alert more than 33,600 victims. This proactive victim-centric approach averted over $204 million of potential losses.

Proactive interventions with potential scam victims

33. To amplify SPF's reach to the community on scam intervention, the ASCom and the Community Policing Units (CPUs) of the Police Land Divisions regularly conduct joint proactive interventions with potential scam victims. These victims were referred by the banks as they attempted monetary transfers observed to be suspicious. In the first half of 2024, more than 140 joint interventions were successfully conducted, further averting more than $36.5 million of potential losses.

International Cooperation and Partnerships

34. Since January 2024, the SPF hosted 36 visits to the ASCom, including visits by overseas law enforcement agencies such as the Royal Malaysia Police, Hong Kong Police Force, Victoria Police and New Zealand Police. The SPF was also invited to present on its anti-scam strategies, particularly the ASC model at 10 international platforms such as the Global Anti Scam Summit in Belgium and the Technical Dialogue on Combating Cyber Scams in Thailand.

Education

35. SPF continues to focus on public education efforts to encourage individuals to proactively adopt anti-scam measures to safeguard themselves and those around them from scams. SPF will also continue to make it easier for members of the public to find information on scams and to seek help.

Availability of anti-scam information and resources via various platforms

"I can ACT against Scams" campaign

36. SPF, supported by the National Crime Prevention Council (NCPC), will continue to work on the "I can ACT against Scams" campaign. The main objective of the campaign is to encourage people to take protective actions to enhance their scam resilience. The campaign promotes three simple anti-scam actions – ADD, CHECK, TELL. In 2023, the campaign promoted the "ADD" part of the framework, encouraging the adoption of security features that helps strengthen the resilience of our devices and online accounts. Key initiatives promoted under the "ADD" phase included adding the ScamShield app, anti-virus app, Money Lock and international call blocking option. For 2024, the campaign will focus on the "CHECK" part of the framework. The key desired behaviour that the campaign seeks to encourage is for individuals to "Stop and Check" before making decisions. This serves as a cognitive break, which will potentially help any individual to better identify the scam situation he or she is in. The campaign will also promote key official resources that the public can check with when they are uncertain if something is a scam.

37. The campaign utilises both out-of-home publicity channels, especially targeting areas with high footfall, as well as digital channels to raise awareness and engagement to the campaign. To further amplify the outreach of the campaign, NCPC has been actively working with various stakeholders such as banks, supermarkets, town councils, and tertiary institutions to disseminate the relevant messages to the

community. NCPC has also been using its social media channels such as Facebook, TikTok, Instagram, WhatsApp and Telegram channels, to reach out to different segments of the society. As of June 2024, NCPC's ScamAlert WhatsApp and Telegram channels have over 35,000 subscribers. The ScamShield app promoted by the "I can ACT against Scams" campaign has reached over 950,000 downloads and users have submitted over 17 million suspected scam SMSes via the app since its launch.

Regular dissemination of information on latest and trending scam types

38. As the scams landscape changes quickly, SPF also ensures a regular cadence of communications on trending scam types and variants to raise public awareness. When there are new scam variants, a Police News Release will be issued. SPF also regularly disseminate scams bulletin and bite-sized videos through social channels such as NCPC's WhatsApp and Telegram channels. Additionally, SPF has been working with SPH on a bi-weekly anti-scam column space which goes out in different vernacular languages.

Harmonising scam-related channels and resources

39. The SPF is also working with partners to make scam related channels and resources more accessible to members of the public, by improving public recall, increase ease in finding information on them, and to encourage greater usage of these resources.

40. In partnership with NCPC and Open Government Products (OGP), the various agencies are working on harmonising the different anti-scam resources under the "ScamShield" brand. The aim is for public's attention to be concentrated on recalling just one brand when it comes to obtaining scam-related information. The ScamShield app was developed to block scam calls and detect scam SMSes. Going forward, the ScamShield brand will be expanded into a suite of anti-scam products, including a new website, an anti-scam helpline (1799), as well as social channels on WhatsApp and Telegram. More details on the harmonisation plans and the new ScamShield suite will be announced in the third quarter of 2024.

SPF Anti-Scam Resource Guide

41. SPF also developed an Anti-Scam Resource Guide which can be found on the SPF website in four vernacular languages. It is also offered to all complainants/victims who lodge scam related reports at Neighbourhood Police Centre counters. The resource guide offers information to frequently asked questions relating to police investigations into scams-related offences and avenues to seek support. The resource guide would be progressively mailed to all Singapore households from the third quarter of 2024.

Rallying the community to fight against scams

42. SPF has been rallying community partners to play a more proactive role in the fight against scams. In collaboration with NCPC and MOM, SPF organised a TikTok challenge in late-2023 to engage migrant workers and migrant domestic workers on scams. Participants from migrant worker communities were challenged to produce creative TikTok videos that helps to raise awareness about scams and scam prevention strategies.

43. SPF has also been engaging industry partners to help amplify public education on scams, in particular for scam types that require targeted outreach. This includes partnering Microsoft on tech support scams, Lalamove on parcel delivery scams, Carousell and ticketing platforms (e.g. TicketMaster, SISTIC and Tickeket) for concert ticket scams. SPF is also working with partners to co-create anti-scam content. For example, SPF partnered META to develop anti-scam content for users of their platforms as well as outreach to youths. Additionally, SPF worked with CirclesLife, StarHub and SingTel to develop anti-scam materials to educate their subscribers.

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

44. The 'Cyber Guardians on Watch' was launched during the Police Workplan Seminar on 24 May 2024 as a holistic effort to tackle a broad range of cybercrimes beyond e-commerce scams. Members of the 'Cyber Guardians on Watch' come from all walks of life and are educated to be SPF's eyes and ears to report any suspicious activity and safeguard our cyberspace. Members will also receive targeted cybercrime-related information, alerts and advisories from the Police through the Police@SG app. They could help to amplify the alert messages by sharing such information with their family and friends. As of 30 June 2024, there were more than 12,000 CWS members in the Cyber Guardians on Watch interest group.

Community Watch Scheme Brunch and Learn

45. The SPF organised the inaugural Community Watch Scheme (CWS) Brunch and Learn event on 24 February 2024. This event brought existing Community Alert System (CAS) subscribers and CWS members together to learn about the latest safety and security concerns. Participants were engaged meaningfully through a mini exhibition, presentations on topics of concern as well as an interactive skit.

Cyber Crime Prevention Ambassador Programme

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

E-commerce Marketplace Transaction Safety Ratings ("TSR")

47. The E-commerce Marketplace TSR was launched in May 2022 to educate consumers on the extent to which different e-commerce marketplaces have put in place safety features in place to protect them from scams.

48. During the latest refresh of the TSR in April 2024, Shopee's rating was upgraded from three ticks to the full four ticks. Similar to other marketplaces which were awarded the full four ticks (i.e., Amazon, Lazada and Qoo10), Shopee has implemented all the safety features deemed critical by MHA. In particular, Shopee has fully implemented user verification against Government-issued documentation for all sellers. The number of reported e-commerce scams on their platform reduced by 65%, from 311 cases in 2022 to 109 cases in 2023.

49. MHA encourages all e-commerce marketplaces to put in place the recommended safeguards, specifically user verification against Government-issued documentation and secure payment options, to protect their users from scams.

WOG Efforts to Fight Scams

Anti-scam measures by the Monetary Authority of Singapore

50. MAS continues to work closely with the financial industry, the Police and other government agencies in the fight against scams. Over the past few years, the banks have implemented a suite of measures to make it harder for scammers to perform unauthorized transactions. Recent measures include:

a. Banks are progressively removing the use of One-Time Passwords (OTP) for bank account login for digital token users to reduce phishing risk.

b. All major retail banks offer a Money Lock feature that allows customers to set aside funds that cannot be digitally accessed. As of 31 July, more than 114,000 customers have utilised Money Lock across major retail banks, with over $9.0 billion of savings set aside.

c. The Association of Banks in Singapore, individual banks and MAS continue to conduct public awareness and education campaigns on scams, to complement national campaigns.

51. As banks continue to tighten anti-scam measures, customers should be prepared for some inconvenience for better security in digital banking and payments. For example, as banks enhance their fraud surveillance capabilities, the rule-based and machine learning algorithms used in fraud surveillance are not precise and may result in more notifications and checks on customers' legitimate transactions.

Anti-scam measures by the Cyber Security Agency of Singapore

52. CSA partnered Google to pilot a new enhanced protection feature within Google Play Protect in February 2024. This feature automatically blocks the

installation of potentially malicious apps from Internet-sideloading sources that use sensitive runtime permissions. The pilot has since been rolled out to all Android devices registered with Google Play Store in Singapore, blocking close to 900,000 high-risk app installations attempts from Internet-sideloading sources on over 200,000 devices. This prevented more than 11,000 apps from potentially being misused for financial fraud and scams, such as impersonating popular messaging, gaming, and e-commerce apps.

53. In March 2024, CSA issued an advisory on how to spot and protect oneself from deepfakes. CSA worked with the SPF and the National Library Board to promote these tips in the SPF's 'Scam or Scram!' mini-video series and the Source.Understand.Research.Evaluate. (S.U.R.E.) festival roadshows, respectively.

54. Since the revamped Be Cyber Safe Pop-Up with interactive games and the Be Cyber Safe Awareness Skit were rolled out to primary and secondary school students in January 2024, they have been staged at 48 primary schools and 47 secondary schools.

55. To reach out to seniors, Be Cyber Safe workshops were held in March and July 2024. These workshops aim to teach seniors how to use digital apps safely via one-on-one guided tutorials by students as well as volunteers from community networks. Workshop partners include banks, Central Provident Fund Board (CPFB), GovTech, the Infocomm Media Development Authority (IMDA) and People's Association. CSA, Singapore Press Holdings (Limited) and Ngee Ann Polytechnic will continue to collaborate on the 'Youth Help Seniors Go Digital' workshops, with accompanying advertorials providing cybersecurity and scam tips running in vernacular publications. The next edition will run from October 2024 onwards.

56. As part of CSA's 'Unseen Enemy' campaign, two roadshows were held in Toa Payoh Hub and Heartbeat@Bedok in February and April 2024 respectively. CSA also engaged Lazada to create a dedicated microsite on their app platform and website to amplify CSA's cybersecurity tips and feature relevant cybersecurity products. In May 2024, CSA also worked with the National Council of Social Service to kickstart a series of talks on cybersecurity and scam awareness for employees and volunteers from over 20 social services agencies.

<u>Anti-scam measures by the Open Government Products</u>

Consolidated single gov.sg SMS Sender ID across government agencies, ministries, statutory boards, and services

57. Since 1 July 2024, the Government has introduced a single SMS Sender ID, gov.sg, which will be used by all government agencies, ministries, statutory boards, and services. Developed by OGP, this consolidation of SMS communications under a single gov.sg SMS Sender ID is a significant step in the government's efforts to protect the public from government official impersonation scams. By using a single gov.sg SMS Sender ID consistently across government agencies, the public can now easily

identify official messages from the government and protect themselves more effectively against government official impersonation scams. This new measure, driven by public feedback on recognizing legitimate government communications, is intended to empower citizens to verify messages from the Government more confidently.

Re-launch of an enhanced ScamShield App

58. Launched on 20 November 2020, the ScamShield mobile application (app) was developed by OGP in collaboration with the SPF and the NCPC. Since its inception, the ScamShield app has had over 950,000 downloads across iOS and Android mobile devices and blocked over 178,000 entities believed to be used for scam calls or SMSes. In a significant stride towards safeguarding the community from a fast-evolving scam landscape, OGP has since enhanced the ScamShield app, which brings together advanced features and functionality for checking, filtering and blocking scam messages and calls, plus scam reporting, to give residents a better way to safeguard themselves against scams. The enhanced ScamShield app can now identify and alert users to potential scam threats across WhatsApp, Telegram and weblinks as well, which offers an added layer of protection from the earlier version of the app that works across calls and SMS only.

Anti-scam measures by the Infocomm Media Development Authority

Working with Telcos to implement anti-scam measures

59. As part of multi-layered measures to protect the public from scams, the IMDA continues to work closely with Telcos to implement anti-scam measures that strengthen safeguards for SMS and calls to Singapore users. Telcos have introduced the international call and SMS blocking features, which provide subscribers with the choice to block both incoming calls and SMSes from international numbers on their mobile phones.

60. By opting in to the feature(s), all incoming calls and/or SMSes made from international numbers will be blocked. Calls and/or SMSes made from Singapore numbers, including users who are roaming overseas, will still be received as per normal. Subscribers can enable and disable the respective features based on their needs.

61. To safeguard against the illicit use of local SIM cards, each individual is only allowed to purchase a maximum of three pre-paid SIM cards today, which is sufficient to meet the needs of genuine users' who are mainly foreign visitors, tourists and contract workers. The SPF and IMDA have observed signs that post-paid SIM cards, predominantly purchased by locals, are increasingly being misused for scams. Therefore, a limit of 10 post-paid SIM cards per individual is imposed. A higher cap is adopted to cater to the needs of legitimate users who may register SIM cards for family members, while limiting illicit usage.

62. This measure took effect from 15 April 2024 and it only applies to new registrations. Subscribers who currently have more than 10 post-paid SIM cards are not affected. However, they will not be able to register additional SIM cards. IMDA will review the post-paid SIM cards limit over time to ensure that it continues to be relevant.

Anti-scam measures by the Central Provident Fund Boad

63. In November 2023, the CPFB introduced a default Daily Withdrawal Limit (DWL) of $2,000 for online CPF withdrawals, for all CPF members aged 55 and above. CPF members who prefer a different DWL could adjust their DWL to any amount from $0 to $200,000, with DWL increases subject to enhanced authentication and a 12-hour cooling period. With effect from 25 September 2024, the maximum DWL will be lowered from $200,000 to $50,000 as part of CPFB's ongoing efforts to strengthen safeguards against scams. This will provide more friction against scams without inconveniencing the majority of members making legitimate withdrawals today.

64. This move is in addition to CPFB's existing safeguards. In December 2023, CPFB introduced enhanced authentication and a 12-hour cooling period when members update their registered bank account with CPFB. Since 29 May 2024, CPF members applying to receive their CPF withdrawals via PayNow will need to set PayNow NRIC-linked bank account as their registered bank account with CPFB.

65. While we seek to strengthen our safeguards, the public continues to play a crucial role in combating scams. This is why CPFB actively engages members through various touchpoints, particularly members reaching withdrawal age of 55 and above, to remind them to stay vigilant and to encourage them to activate the CPF Withdrawal Lock if they have no intention to withdraw their CPF savings soon. For more details on CPF's anti-scam security measures, please visit cpf.gov.sg/antiscammeasures.

Strengthening legislative levers

The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Computer Misuse Act (CMA)

66. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Computer Misuse Act (CMA) were amended in May 2023 and new offences were introduced to make it easier for the SPF to make out a money laundering offence and allow the SPF to deal with individuals who abuse their Singpass credentials. The amendments took effect on 8 February 2024 and the Sentencing Advisory Panel Guidelines for the new offences were published on 21 August 2024, which may be accessed at sentencingpanel.gov.sg/guidelines-for-scams-related-offences.

Amendments to Miscellaneous Offences Act to criminalise the misuse of local SIM cards

67. Criminal syndicates are increasingly using local SIM cards to perpetrate scams, including to receive scam monies (e.g., via PayNow) and to set up messaging accounts (e.g., WhatsApp/Telegram). The number of local mobile lines involved in

scams and other cybercrimes quadrupled from 5,867 in 2021, to 23,519 in 2023, while losses almost tripled, from $137 million to $384 million.

68. To address this problem, the Law Enforcement and Other Matters (LEOM) Bill was passed in Parliament on 2 April 2024 to amend the Miscellaneous Offences Act, to enhance our abilities to enforce against criminals who abuse local SIM cards to perpetrate scams. These include, among others:

a. Registering for a SIM card and selling it for gain;

b. Possessing a large number of unregistered SIM cards for no legitimate reason; and

c. Buying or selling SIM cards registered in another person's particulars.

69. The offences will carry a fine of up to $10,000 or imprisonment of up to three years, or both. For (b) and (c), the penalty for a second or subsequent offence will be a fine of up to $20,000 or imprisonment of up to five years, or both.

Progressive operationalisation of the Online Criminal Harms Act

70. The Online Criminal Harms Act (OCHA), which has been progressively operationalised since 1 February 2024, allows the authorities to direct online service providers or other entities to disable access to online criminal content or accounts, including scams.

71. Under OCHA, two Code(s) of Practice (COP) took effect on 26 June 2024, one for Online Communication Services and another for E-Commerce Services[1]. Providers of designated online services, which present the highest risk of scams to Singapore users, are required to put in place upstream measures to proactively prevent and disrupt scams (e.g. user verification against Government-issued records to tackle e-commerce scams). SPF will work closely with the providers of designated online services and monitor their compliance to the COPs.

<u>Upcoming measures to better protect scam victims</u>

72. MHA is studying measures to better protect scam victims, particularly those who do not believe that they are being scammed. These could be victims of love scams or investment scams who have invested their emotions or significant amounts of monies, making it difficult for them to extricate themselves from the situation.

73. Specifically, MHA is considering to empower Police officers to restrict the banking transactions of scam victims and targets of ongoing scams, if there is reasonable belief that they will make money transfers to scammers. The restriction will be time-limited, as the intent is to give the Police time to convince the victims that they

[1] This includes online services that facilitate e-commerce activities.

are being scammed. MHA intends to conduct public consultations on our proposals. More details will be released when ready.

Everyone Plays a Part in Fighting Scams

74. Everyone has a part to play in keeping Singapore safe and secure. Individuals should proactively adopt anti-scam measures to safeguard themselves and those around them from scam. SPF will continue to work with government agencies and community partners to engage and educate the public in building the community's vigilance and resilience towards scams. In addition, business operators, particularly banks, online marketplaces and telcos, also 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.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
22 AUGUST 2024 @ 3PM

Annex

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

Types of Scams	Cases reported		Total amount lost (at least)		Average amount lost in first half of 2024
	Jan - Jun 2024	Jan - Jun 2023	Jan - Jun 2024	Jan -Jun 2023	
E-commerce Scams	7,250	4,496	$8.6M	$7.3M	$1,191
Job Scams	5,717	5,723	$86.0M	$78.3M	$15,055
Phishing Scams	3,447	2,948	$13.3M	$7.3M	$3,868
Investment Scams	3,330	1,577	$133.4M	$80.4M	$40,080
Fake Friend Call Scams	2,368	3,832	$8.1M	$12.9M	$3,426
Government Officials Impersonation Scams	580	367	$67.5M	$40.4M	$116,534
Loan Scams	571	426	$2.5M	$2.5M	$4,459
Internet Love Scams	418	435	$12.5M	$25.7M	$29,969
Offer Sexual Services Scams	410	168	$1.9M	$439K	$4,780
Social Media Impersonation Scams	347	508	$1.8M	$4.4M	$5,454
Top 10 scams	**24,438**	**20,480**	**$336.1M**	**$260.2M**	**$13,754**

Note: Total amount cheated may not tally due to rounding.