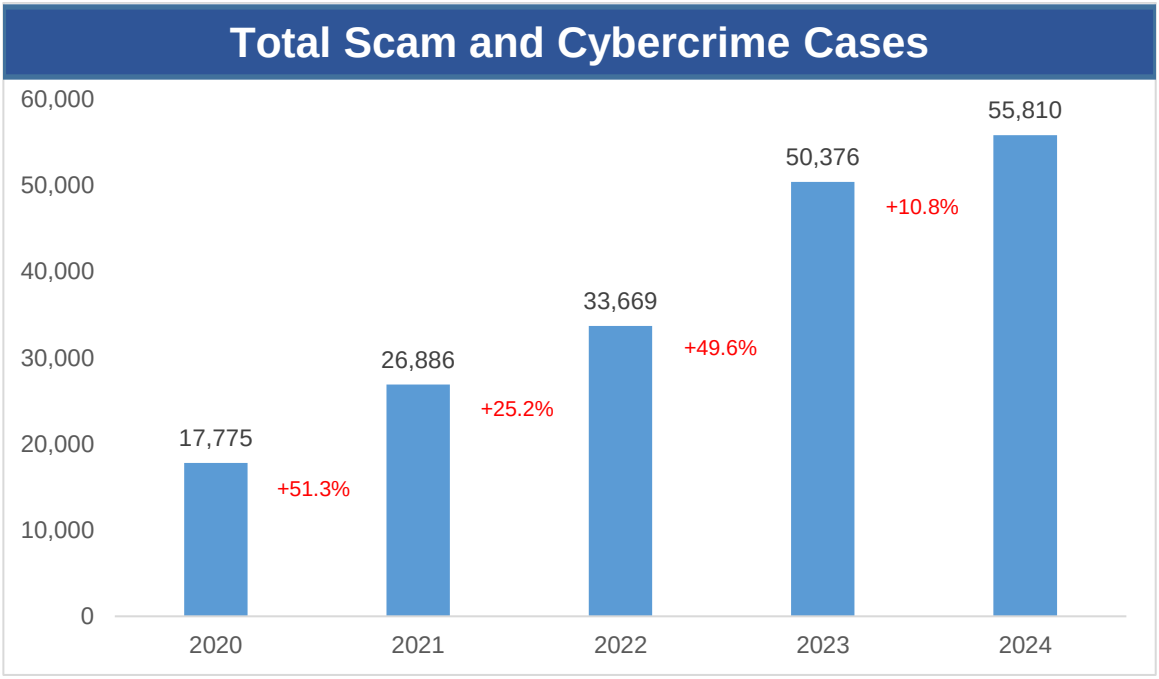
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Annual Scams and Cybercrime Brief 2024

Overall Scams and Cybercrime Situation in 2024

Scams and cybercrime remain a pressing concern. In 2024, the **number of scam and cybercrime cases increased by 10.8% to 55,810 cases**, compared to 50,376 cases in 2023.

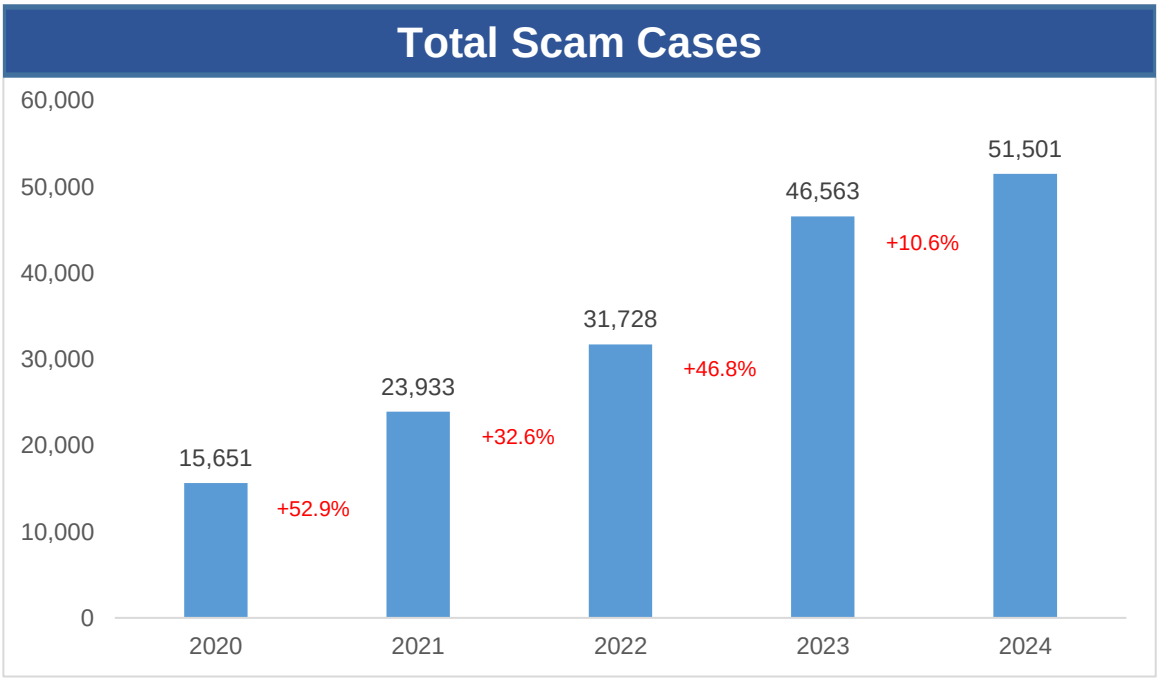


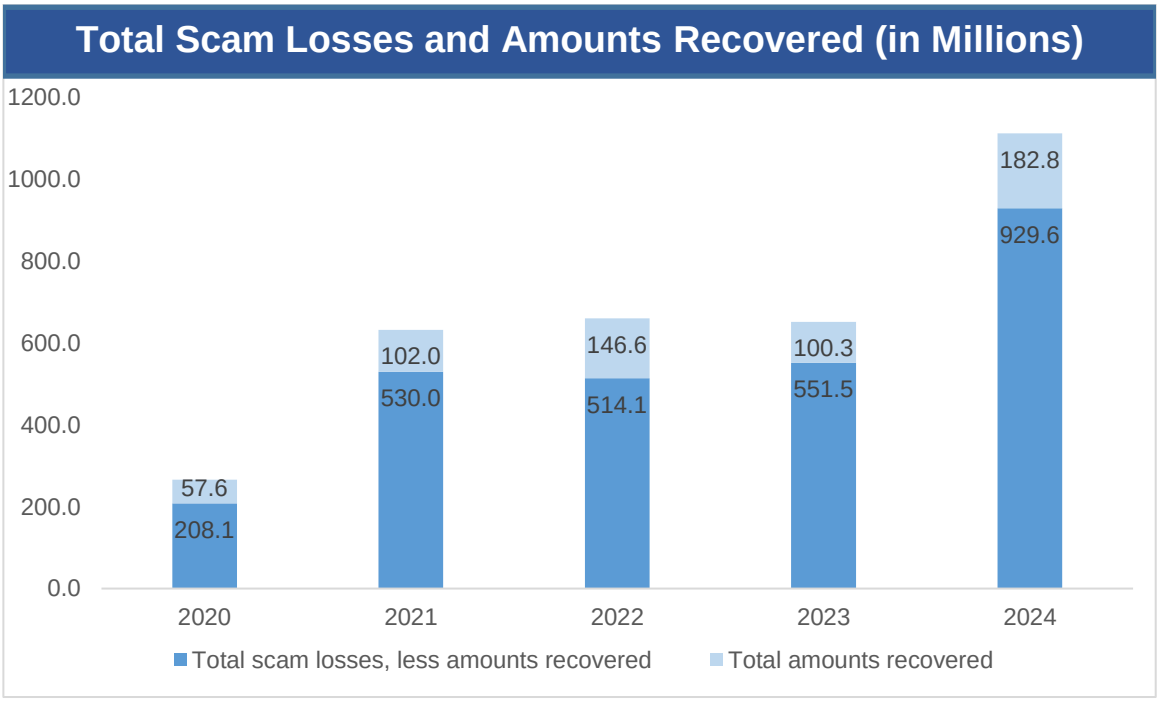
2. Scams accounted for 92.3% of these 55,810 cases. The **total number of scam cases increased by 10.6% to 51,501 cases in 2024**, from 46,563 cases in 2023. The **total amount lost increased by 70.6% to at least $1.1 billion in 2024**, from at least $651.8 million in 2023.

3. **In 2024, the Anti-Scam Command (ASCom) successfully recovered more than $182 million of scam losses, and the net scam losses was about $930 million.** In addition, through proactive interventions with victims at various stages of being scammed, ASCom and its partners had **averted at least $483 million in potential losses.**

4. **Cryptocurrency losses formed a larger percentage of scam losses, accounting for about 24.3% of total scam losses in 2024**, compared to about 6.8% of total scam losses in 2023.

5. There were **significant decreases** in both the number of cases reported and total amount lost for **fake friend call scams**. There were also **notable decreases** in the number of **malware-enabled scams** and **social media impersonation scams** largely as a result of several measures implemented by the Government and stakeholders like the banks and telcos, though there were increases in the total amount lost to these two scam types due to two cases with very high losses.

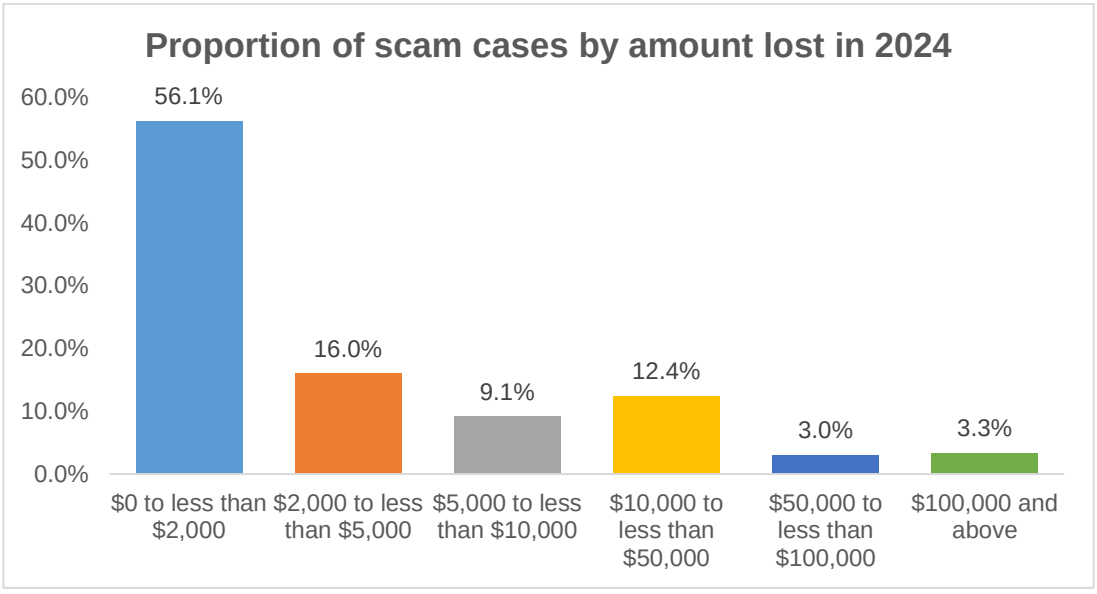




6. **On the other hand, there were increases in e-commerce scams, phishing scams, investment scams, and government official impersonation scams.**

7. **The majority of the cases, more than 70%, saw less than $5,000 in losses. The median loss per case fell 12.6% from $1,590 in 2023 to $1,389 in 2024.**

8. **The increase in total amount lost was driven by a small number of cases with very high losses (details in Annex B).** Scam cases with losses of at least $100,000 made up 3.3% of the scam cases in 2024, but 70.8% of the scam losses. Four cases accounted for $237.9 million in losses.

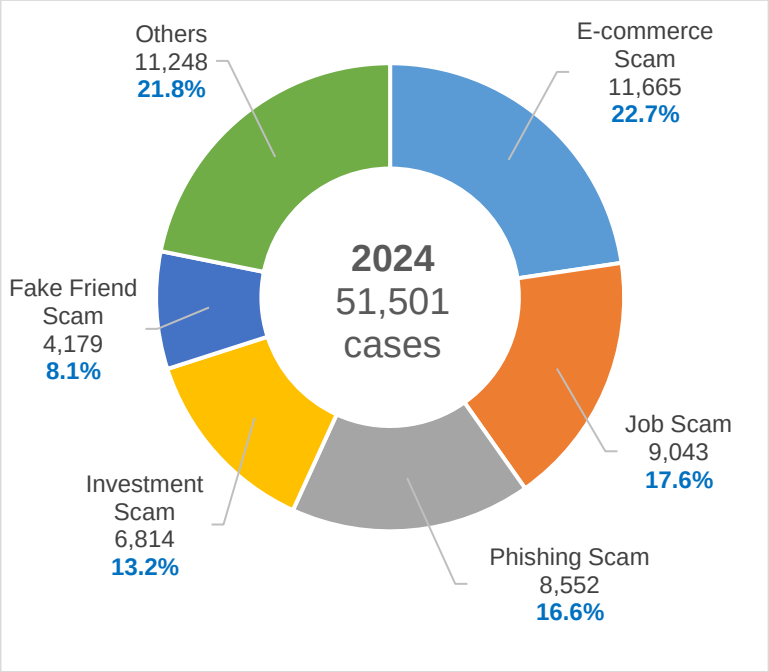


9. **In 2024, self-effected transfers accounted for 82.4% of total reported scam cases**. In most of these cases, the scammers did not gain direct control of the victims' accounts, but manipulated victims into performing the monetary transactions, by means of deception and social engineering.

Scam and Cybercrime Types of Concern

10. In terms of case numbers, **e-commerce scams, job scams, phishing scams, investment scams and fake friend call scams** were the top five scam types in 2024**.**

Breakdown of scam types by number of cases



11. In terms of the total amount lost, **investment scams, job scams, government officials impersonation scams, malware-enabled scams, and business email compromise scams** were the top five scam types in 2024.

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

12. 2024 saw **sharp increases** in both the number of cases reported and the amount lost for **phishing scams**, **investment scams, and government officials impersonation scams**.

a) E-commerce scams

i. E-commerce scams recorded the highest number of reported cases among all scam types in 2024, with 11,665 cases reported and at least $17.5 million lost. Concert tickets was the top item involved in e-commerce scams.

ii. The majority of e-commerce scam victims were aged 30 to 49, accounting for 45.1% of victims for this scam type. The most common platforms on which e-commerce scams were conducted included Facebook, Carousell, and Telegram.

b) Investment scams

i. Investment scams recorded the fourth highest number of reported cases among all scam types in 2024, with 6,814 investment scam cases reported. The total amount lost to investment scams in 2024, on the other hand, is the highest amongst the various scam types, at least $320.7 million. The Police would like to highlight an approach which saw increased prevalence in 2024, where victims were added into

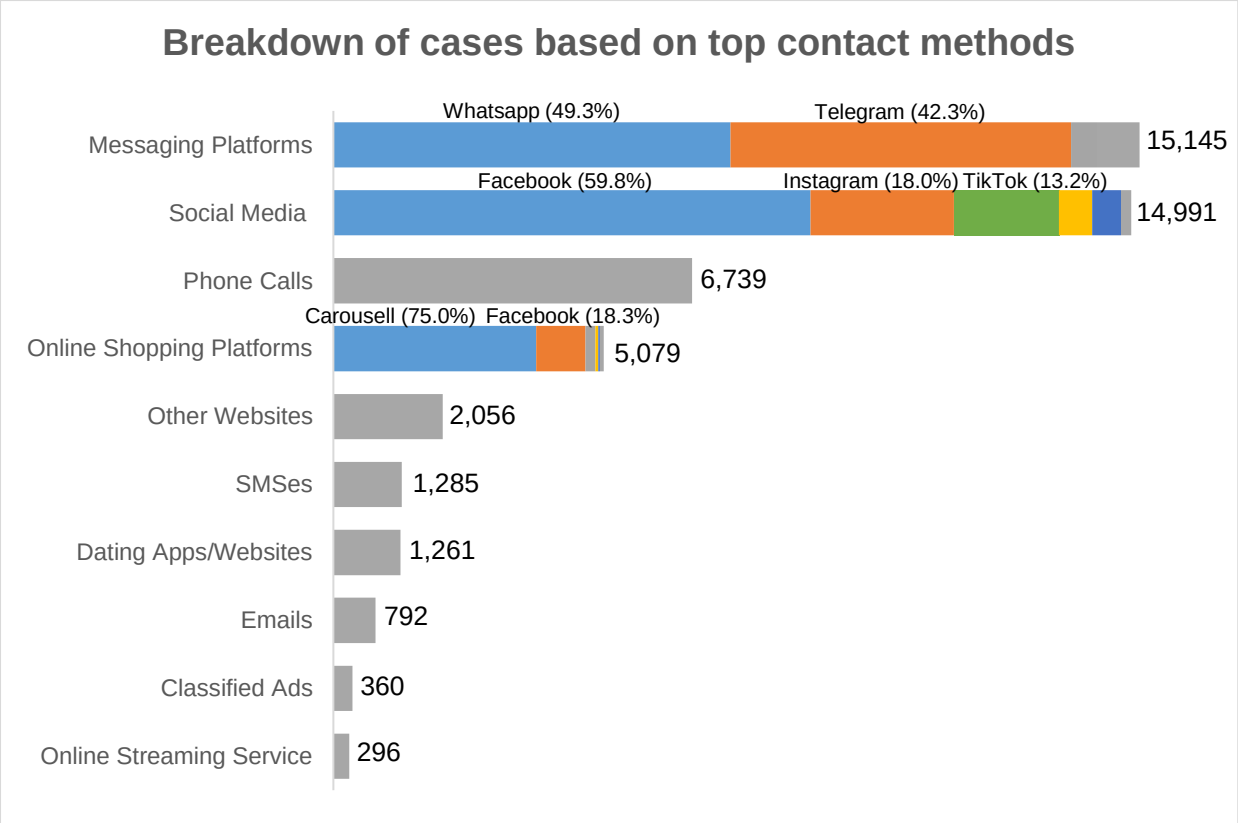
chatgroups or channels via messaging platforms such as WhatsApp and Telegram by scammers for purported “investment opportunities”.

ii. The majority of investment scam victims were aged 30 to 49, making up 44.2% of victims for this scam type. Telegram, Facebook and WhatsApp were the most common platforms used by investment scammers to contact potential victims.

Top Contact Methods

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

14. **Three products from Meta (Facebook, WhatsApp, Instagram) and Telegram 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 2024.



Messaging Platforms

15. In 2024, messaging platforms were the most common means by which scammers contacted victims. The number of cases where scammers contacted

victims via messaging platforms increased to 15,145 from 12,368 in 2023. **WhatsApp and Telegram were the top two messaging platforms exploited by scammers**.

16. **The number of scam cases perpetrated on Telegram saw an increase of about 95.7% in 2024.**

Social Media Platforms

17. The number of scam cases where scammers contacted victims via social media increased to 14,991 in 2024, from 13,725 in 2023. In particular, 59.8% were contacted through Facebook, 18.0% were contacted through Instagram, and 13.2% through TikTok**.**

Online Shopping Platforms

18. Online shopping platforms is a contact method of concern. The number of scam cases perpetrated via online shopping platforms increased to 5,079 in 2024, from 4,893 in 2023. In particular, 75.0% of these cases occurred on Carousell, and 18.3% on Facebook Marketplace.

Scam Victim Profile

19. **In 2024, 70.9% of scam victims were youths, young adults, and adults aged below 50. As for the elderly, while they made up only a small proportion of the scam victims, the average amount they lost per victim is 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 6.3% of scam victims. 38.4% fell prey to e-commerce scams, while 20.2% fell prey to job scams and 15.3% fell prey to phishing scams. Scammers tend to contact youths via messaging platforms, social media and online shopping platforms.

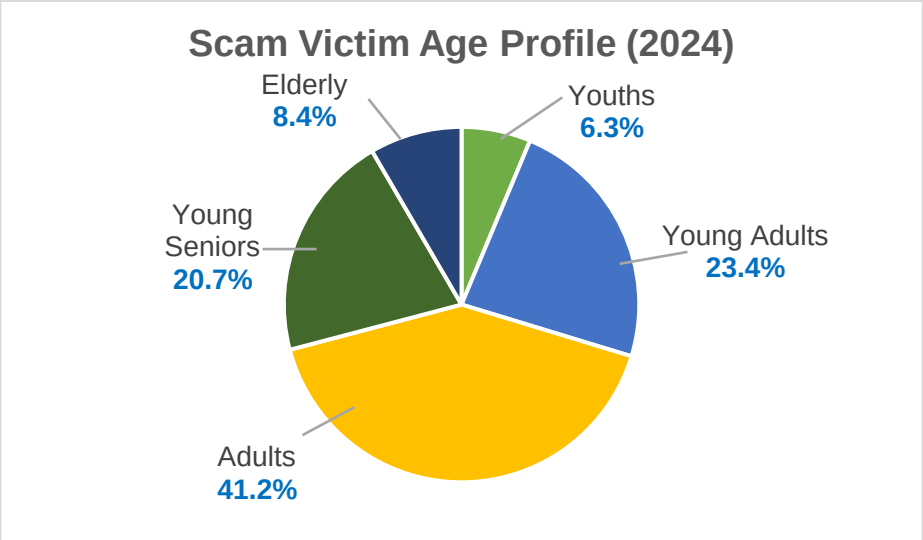
b) Young adults, aged 20 to 29, made up 23.4% of scam victims. 33.2% fell prey to e-commerce scams, while 22.1% fell prey to job scams and 13.0% fell prey to phishing scams. Scammers tend to contact young adults via messaging platforms, social media and online shopping platforms.

c) Adults, aged 30 to 49, made up 41.2% of scam victims. 25.5% fell prey to e-commerce scams, while 18.9% fell prey to job scams and 17.2% fell prey to phishing scams. Scammers tend to contact this victim group via social media, messaging platforms and online shopping platforms.

d) Young seniors, aged 50 to 64, made up 20.7% of scam victims. 19.7% fell prey to phishing scams, while 18.6% fell prey to investment scams and 14.1% fell

prey to fake friend call scams. Scammers tend to contact this victim group via social media, messaging platforms and phone calls.

e) The elderly, aged 65 and above, made up 8.4% of scam victims. 19.5% fell prey to phishing scams, while 19.3% fell prey to investment scams and 18.7% fell prey to fake friend call scams. Scammers tend to contact the elderly via messaging platforms, phone calls and social media.



Police's Efforts to Fight Scams and Cybercrimes

Enforcement

Strengthening legislative levers

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

20. 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 curb the facilitation of scams and the movement of criminal proceeds, as well as the abuse of Singpass. Since the amendments took effect on 8 February 2024, Police have been charging the accused persons in Court under the new offences for scams-related money mule activities.

21. The Sentencing Advisory Panel guidelines for the new offences were published on 21 August 2024.[1] The Guidelines recommended that significant imprisonment terms be the norm for scams-related offences. For example, the recommended starting sentence is six months' imprisonment for negligently handing over control of

[1] The Guidelines can be accessed at https://www.sentencingpanel.gov.sg/guidelines-for-scams-related-offences

one's bank account to another person; and 18 months' imprisonment for handing over control of a bank account to another person knowing or having reason to believe that this would assist the person in retaining criminal proceeds.

22. The Courts have started applying the sentencing guidelines published by the Sentencing Advisory Panel, and imposed significant imprisonment terms on money mules and others who facilitate scams.

a) In one concluded case, the offender received RM1,000 for sharing access of his internet banking account with another person, without taking reasonable steps to ascertain the purpose of this arrangement. The bank account was then used to launder more than $160,000 of criminal proceeds. The offender was convicted and sentenced to six months' imprisonment and was required to disgorge the unlawful gain made from the arrangement.

b) In another case, the offender accepted an offer of "fast cash" of $2,400 in exchange for allowing an unknown person to control his Singpass account. The offender's Singpass identity was thereafter used to open two bank accounts which were used to receive more than $337,000, of which at least $114,000 were from 21 scam victims in Singapore. The offender was convicted and sentenced to eight months' imprisonment and was required to disgorge the unlawful gain made from the arrangement.

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

23. 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). To address this problem, the Law Enforcement and Other Matters (LEOM) Bill was passed in Parliament on 2 April 2024 and came into effect on 1 January 2025, to amend the Miscellaneous Offences Act, enhancing our abilities to enforce against those who abuse local SIM cards to perpetrate scams:

a) **[Group A]** Irresponsible SIM card subscribers, who give away their local SIM cards, or provide their particulars to others to be used to sign up for local SIM cards;

b) **[Group B]** Middlemen involved in procuring or providing local SIM cards to scam syndicates; and

c) **[Group C]** Errant retailers who facilitate fraudulent local SIM card registrations.

24. The offences carry a fine of up to $10,000 or imprisonment of up to three years, or both. For Groups B and C, the penalty for a second or subsequent offence is a fine of up to $20,000 or imprisonment of up to five years, or both.

Operationalisation of the Online Criminal Harms Act

25. 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 disrupt online criminal content and activities, including scams.

26. 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[2]. 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.

a) The COP for Online Communication Services is applicable to five designated services: Facebook, WhatsApp, Instagram, Telegram, and WeChat. The Online Communication Code requires these designated online services to implement appropriate systems, processes or measures to achieve the following:

    i. Quick disruption of malicious accounts and activities, such as proactively detecting and taking necessary action against suspected scams and malicious cyber activities;

    ii. Deployment of safeguards to prevent the propagation of malicious activities such as reasonable verification measures to prevent the creation and use of inauthentic accounts; and

    iii. Accountability of online service providers, where an annual report on the implementation of the systems, processes and measures to meet the above two outcomes has to be submitted.

b) The COP for E-commerce Services is applicable to four online services which facilitate e-commerce activities and pose the highest risks of e-commerce scams to Singapore users: Facebook Marketplace, Facebook Advertisements, Facebook Pages, and Carousell. The E-commerce Code has the same requirements as the Online Communication Code, with two additional requirements which the Ministry of Home Affairs (MHA) has assessed to be critical in safeguarding against e-commerce scams:

    i. To subject users who advertise or post about the sales of goods and/or services, or those who intend to do so, to verification against Government-issued records; and

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

ii. To provide, as an option for users, payment protection mechanisms that require delivery of goods or services to be verified, before payment is released to the sellers.

Passing of the Protection from Scams Bill in Parliament

27. Despite the various banking measures implemented (e.g., Money Lock and kill-switch) and extensive public education efforts over the years, the number of scams involving self-effected transfers - where individuals willingly transfer monies to scammers - remains high (82.4% of total reported scam cases in 2024). In some of these cases, the individuals were so taken in by the scammers' deceit, that they refused to believe that they were being scammed despite repeated advice from loved ones, their bank, and even the Police.

28. In January 2025, Parliament passed the Protection from Scams Bill. The Bill 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. This will give the Police more time to engage and convince the individual that he or she is being scammed.

29. The Protection from Scams Act will be operationalised in 2025.

<u>Law enforcement interventions and operations</u>

Enforcement operations against scammers and money mules

30. **In 2024, the ASCom, together with the Scam Strike Teams in the seven Police Land Divisions, conducted 25 island-wide anti-scam enforcement operations, leading to the investigation of more than 8,000 money mules and scammers.** Police have charged more than 660 scammers and money mules in Court, including more than 110 of them under the new laws of the CDSA and CMA.

Enforcement operations against the misuse of SIM cards

31. ASCom launched a series of enforcement operations in 2024 to address the misuse of SIM cards in scam activities. These included crackdowns on unscrupulous SIM card retailers who had abused their position by registering additional SIM cards under their customers' names without the customers' awareness or permission, and actions against individuals and criminal organisations offering One-Time-Password (OTP) services for activating messaging and chat applications. These illegal OTP services utilised mobile numbers associated with pre-registered SIM cards.

32. **These operations resulted in the seizure of over 31,000 SIM cards and the arrest of 13 individuals**, including two Malaysian runners who were linked to a syndicate operating in Malaysia, who allegedly procured prepaid SIM cards from convenience stores in Singapore and brought them back to Malaysia for the

syndicate's illicit activities. **Two retailers were also arrested, for their suspected involvement in fraudulent registration of prepaid/postpaid SIM cards**, and one of them has since been charged in Court in January 2025.

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

33. The SPF collaborated with Government Technology Agency of Singapore (GovTech) and HTX (Home Team Science and Technology Agency) to develop the Scam Analytics and Tactical Intervention System (SATIS), which leverages artificial intelligence and machine learning to triage, assess and disrupt scam-related websites swiftly. A similar system called SATIS+ was built to disrupt online monikers, with planned improvements to disrupt other scam enablers such as payment channels and mobile numbers.

34. **In 2024, the SPF disrupted more than 57,700 mobile lines, more than 40,500 WhatsApp lines, more than 33,600 online monikers and advertisements, and more than 44,900 websites that were scam-related**. This is a significant increase in disruptions as compared to 2023, and was done through collaborations with major industry stakeholders such as Meta, Carousell, Google and the telecommunications companies.

Disrupted asset	2023	2024	% increase
Mobile lines	> 9,200	> 57,700	> 527%
WhatsApp lines	> 29,200	> 40,500	> 38%
Online monikers and advertisements	> 4,100	> 33,600	> 719%
Websites	> 25,000	> 44,900	> 79%

35. The ASCom has also expanded its partnerships to more than 120 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 2024, the ASCom froze more than 21,000 bank accounts based on reports referred to the ASC and recovered more than $182 million**.

36. In particular, the co-location initiative was expanded to include the co-location of Carousell and Shopee staff within ASCom in 2024. This initiative was instrumental

in supporting ASCom in swift intervention in scam cases on these platforms and proactively detecting and taking down scam-tainted online monikers and suspicious advertisements.

Collaboration with foreign law enforcement agencies

37. Most online scams are perpetrated by scammers based outside of Singapore, making such cases difficult to investigate and prosecute. The 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.

Takedown of scam syndicates through collaboration with overseas law enforcement agencies

38. **In 2024, the close collaboration between the SPF and overseas law enforcement agencies resulted in the successful takedown of 16 transnational scam syndicates** comprising four fake friend call syndicates, eight suspected money laundering cells, one phishing scam syndicate, one technical support scam syndicate, one business email compromise scam syndicate, and one investment scam syndicate. More than 150 persons based overseas who were responsible for more than 2,300 transnational scam cases involving losses of more than $58 million, were arrested.

39. Fake friend call scams recorded a decrease of 39.1% in cases, with a 41.1% decrease in losses in 2024. 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.

Participation in internationally coordinated scam operations

40. The SPF participated in INTERPOL's Operation HAECHI V, where more than 1,600 subjects involved in scams were investigated and more than 5,100 bank accounts were blocked, seizing more than $54.8 million. More than 1,000 virtual accounts were blocked, resulting in the seizure of more than $798,000 in virtual assets.

International cooperation for asset recovery

41. In July 2024, a Singapore commodities firm fell prey to a Business Email Compromise Scam and paid US$42.3 million (approximately $57.2 million) to a fraudulent bank account in Timor-Leste. Swift actions by the ASC, INTERPOL and Timor-Leste authorities led to the interception of US$39.3 million. Further investigations resulted in nine arrests and the recovery of an additional US$2.7 million.

42. **In October 2024, the SPF formalised "FRONTIER+" with the anti-scam units of five countries and jurisdictions, namely Hong Kong SAR, Malaysia, Maldives, South Korea and Thailand, to galvanise an alliance to step up collective efforts in asset recovery.** FRONTIER+ seeks to enhance collaboration in disrupting scammers' operations, mitigating financial losses for victims, and fostering capability building through the sharing of best practices. This initiative will significantly strengthen international efforts in combating cross-border scams and recovering illicitly transferred funds. Through this network, the ASC assisted Malaysia's National Scam Response Centre to recover more than RM378,400 linked to a case of investment scam in December 2024.

Engagement

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

43. 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 six joint operations in 2024 between ASC and the partnering banks, more than 77,100 SMSes were sent to alert more than 55,600 victims. **This proactive victim-centric approach averted over $420 million of potential losses**.

Proactive interventions with potential scam victims

44. 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 financial institutions as they had attempted monetary transfers observed to be suspicious. **In 2024, more than 550 such interventions were conducted, averting more than $63.3 million of potential losses**.

Education

45. 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.

Increasing accessibility to self-help anti-scam resources

Launch of ScamShield Suite

46. The SPF, the National Crime Prevention Council (NCPC) and Open Government Products (OGP) jointly launched the ScamShield Suite on 27 September 2024.

47. ScamShield was expanded from an app to a suite of four anti-scam resources which aims to enable members of the public to better protect themselves against scams by – (a) providing a one-stop solution for members of the public (MOPs) to access scam-related information; (b) improving ease and speed with which MOPs can find information on scams; (c) improving public recollection and understanding of the resources; and (d) increasing usage of these anti-scam resources:

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

ii. Enhanced ScamShield app – Block scam calls and detect scam SMSes; check if something is a scam; share information on scam encounters with authorities;

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

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

48. Since the launch of the ScamShield Suite, the usage and adoption of anti-scam resources have increased significantly. NCPC's anti-scam helpline previously received approximately 14 calls a day in 2023. **The newly launched 24/7 ScamShield helpline currently receives around 500 calls daily. The ScamShield app saw an increase in downloads from 944,000 before the launch of the enhanced app, to over 1.18 million downloads.** The ScamShield Alert social media channels saw an increase from 35,000 subscribers to 78,800 subscribers, and the new ScamShield website has been visited by over 1.2 million visitors since the launch.

Raising awareness on anti-scam protective measures and on scam types

"I can ACT against Scams" campaign

49. 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.

50. From November 2024, the new phase of the campaign focused on the "Check" part of the framework, to encourage individuals to "Stop and Check" before making monetary transfers and making decisions related to such. This encourages and 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 will promote key official resources that the public can check with when they are uncertain if something is a scam.

Anti-scam publicity via targeted media campaigns

51. In addition to the timely dissemination of information on the latest scam trends, the SPF has been working with media agencies on monthly media campaigns to promote the public's awareness of 'high loss' scam types like government official impersonation scams, investment scams and job scams, targeted at demographic segments vulnerable to these scam types. For example, for seniors, who are more vulnerable to government official impersonation scams, content on this scam type was incorporated in targeted channels popular with the elderly, such as SPH's getai platforms, Jack Neo's 2025 Chinese New Year Movie "I Want To Be Boss" and radio commercials on YES933 and Class95. Examples of other channels and platforms utilised for the monthly media campaign include Mothership, RICE media, TheSmartLocal, The Woke Salary Man, and AsiaOne.

<u>Rallying the community to fight against scams</u>

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

52. The SPF has been engaging community and industry partners to help amplify public education on scams. By tapping on their networks, the SPF was able to reach out more effectively to different population segments. For example, the SPF worked with Mummy Yummy, a network of volunteers delivering food to elderly beneficiaries, to weave in anti-scam topics in their engagements with their beneficiaries. The SPF partnered the Federation of Merchants' Association to distribute coffee cups with the ScamShield helpline number, starting with a pilot at Boon Lay Hawker Centre in October 2024. Another partnership was with Amazon, who assisted to distribute scam pamphlets in their packages, and printed anti-scam messages on their packages. The SPF has also been working with partners to co-create anti-scam content. For example, SPF and NCPC partnered with Eyeyah and Meta, to jointly produce an anti-scam public education magazine for youths, which featured engaging visuals and interactive activities to educate youths on common scam signs and protective actions to take against scams.

#XiamTheScams web game by NCPC

53. The #XiamTheScams web game was launched on 24 October 2024 by the NCPC. The game, which concluded on 22 January 2025, engaged over 519,000 players over the three-month long game period. Designed as a fun, educational, and easy-to-play life simulator, the game sought to raise public awareness of common scams in Singapore and anti-scam protective measures. Players navigated real-life-inspired scenarios, and made strategic decisions to overcome challenges, while learning to identify and avoid scams.

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

54. The 'Cyber Guardians on Watch' was launched during the Police Workplan Seminar on 24 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 on 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 31 December 2024, there were more than 32,000 members in the Cyber Guardians on Watch interest group.

Cyber Crime Prevention Ambassador Programme

55. 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. The Cyber CPAs has since reached out to more than 8,000 members of the public across 21 events over the past six months.

E-commerce Marketplace Transaction Safety Rating

56. 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.

57. 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. Specifically, several e-commerce marketplaces which have implemented the recommended safety features under the TSR (e.g. Amazon, Lazada) have seen significantly fewer scams than other platforms.

Whole of Government Efforts to Fight Scams

Anti-scam measures by the Monetary Authority of Singapore

58. MAS continues to collaborate with the financial industry, the Police and other Government agencies in implementing collective defences against scams.

59. To further address phishing risks, the major retail banks have phased out the use of One-Time Passwords (OTP) for bank account logins by digital token (DT) users, further protecting users from unauthorised access to their bank accounts. They have also implemented Singpass Face Verification for higher risk scenarios in the DT setup process, in addition to the 12-hour cooling period for DT setup. This will make it more difficult for a scammer to take over a customer's DT by setting it up on his own device.

60. Since its introduction in November 2023, usage of the Money Lock[3] feature has risen as banks improve the ease and convenience for funds to be placed under Money Lock. As at 31 December 2024, more than 245,000 customers have utilised Money Lock, with close to $20.9 billion of savings set aside. From February to March 2024, the SPF, NCPC and MAS jointly ran a publicity campaign which utilised both social media and out-of-home channels to raise awareness and encourage the adoption of Money Lock. Banks will also continue publicity efforts to encourage their customers to use Money Lock, especially among the elderly.

61. On 16 December 2024, MAS and the Infocomm Media Development Authority (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.

62. MAS will continue to work with financial institutions on anti-scam measures as the threat landscape evolves. As this could inevitably introduce more notifications and checks on legitimate transactions, customers should be prepared for some inconvenience in digital banking and payments, in exchange for enhanced security.

Anti-scam measures by the Cyber Security Agency of Singapore

63. In February 2024, the Cyber Security Agency of Singapore (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 December 2024, the EFP feature

---

[3] Money Lock provides added protection against digital scams by allowing the customer to block online access to a portion of their funds, should their digital banking access be compromised.

has successfully blocked 1.6 million installation attempts of potentially malicious applications across 370,000 devices. This prevented 25,000 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.

64. CSA's 'Unseen Enemy' national campaign continued into its second year, utilising a combination of out-of-home platforms, free-to-air TV channels, and digital platforms to amplify messages featuring four cyber tips. A 6th campaign is in the works and will be launched in the second half of 2025.

65. In January 2025, CSA released a new list of recommended security apps to help members of the public identify suitable apps to download to better safeguard their mobile devices against phishing and malware attacks.

66. To reach out to seniors, CSA continues to run the Be Cyber Safe workshops in community centres, where seniors learn how to use digital apps safely via guided tutorials by students as well as volunteers from community networks. CSA, Singapore Press Holdings (Limited) and Ngee Ann Polytechnic continue its collaboration on the 'Youth Help Seniors Go Digital' workshops, with accompanying advertorials providing cybersecurity and scam tips running in vernacular publications. The workshops will run from October 2024 to April 2025.

67. CSA collaborated with Microsoft to conduct workshops for primary and secondary school students to encourage adoption of good cyber hygiene practices through gamification. These workshops leveraged Microsoft's Minecraft education cybersecurity modules to bring across cybersecurity messages using immersive scenarios in the Minecraft world. Since the rollout in September 2024, CSA has conducted these workshops for 12 schools, and more than 40 other schools have registered their interest.

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

68. Since 1 July 2024, the Singapore Government has implemented a single SMS Sender ID, 'gov.sg', for all government agencies. This replaces 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.

Enhanced ScamShield App

69. OGP enhanced the ScamShield App in August 2024 to expand ScamShield's protection from passive to active to combat emerging scam variants, so as to enable users to protect themselves by actively checking suspicious messages, calls and websites occurring on third-party platforms such as WhatsApp and Telegram. The enhanced app simplifies reporting, for more crowdsourced data to improve scam

protection and scam intelligence, which in turn improve our classifier performance to make sure scam calls and SMSes are detected accurately.

70. Since the enhanced app was launched, there has been a 25% growth in the app user base from 944,000 to 1.18 million users currently. More than 180,000 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.

Anti-scam measures by the Infocomm Media Development Authority

Feature to block international calls and SMSes

71. As part of the multi-layered measures to strengthen protection for members of the public against scams coming through telecommunication networks, IMDA worked with the telecommunications companies last year to offer subscribers the feature to block all incoming calls and/or SMSes from international numbers on their mobile phones.

72. To date, over 287,000 subscribers have activated the feature to block calls from international numbers, while over 219,000 subscribers have activated the feature to block SMS from international numbers.

Feature extended to residential fixed lines

73. From 31 Dec 2024, residential fixed line subscribers of key operators (namely M1, SIMBA, Singtel, StarHub, and MyRepublic) were also able to activate this feature for fixed line voice services. From 14 March 2025, this will be extended to all other mobile and residential fixed line providers, such as Circles.Life and RedOne. Subscribers are encouraged to check with their respective telecommunications companies to activate the features.

Anti-scam measures by the Central Provident Fund Board

74. In September 2024, the maximum Daily Withdrawal Limit (DWL) for online CPF withdrawals was lowered from $200,000 to $50,000. This provides more friction against scams and introduces more time between transactions to prevent further losses, without inconveniencing the majority of members making legitimate withdrawals. The amount withdrawable by CPF members aged 55 and above remains unchanged, and is subject to the current withdrawal rules.

75. In December 2024, to complement WOG efforts in tackling government officials impersonation scams which typically involve unsolicited calls, the Central Provident Fund Board (CPFB) consolidated all outbound calls under 6227 1188 or 6202 3388. These numbers are published on CPFB’s website (cpf.gov.sg/antiscamtips), whitelisted in ScamShield, and publicised on CPFB’s advisories and social media platforms, to allow members to verify calls from the Board. Additionally, if members

missed a call from CPFB, they would receive a gov.sg SMS or email notification with callback details.

76. The above measures are in addition to CPFB's existing suite of anti-scam measures, which includes the CPF Withdrawal Lock, as well as enhanced authentication and a 12-hour cooling period for making any changes to the DWL, registered bank account information or contact details.

77. The CPFB also actively engages members through various touchpoints, particularly members 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.

Everyone Plays a Part in Fighting Scams

78. 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, individuals are encouraged to check with someone they trust, call the ScamShield Helpline at 1799, or check the ScamShield app.

79. 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
25 FEBRUARY 2025 @ 3PM

Annex A

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 2024
	2024	2023	2024	2023	
E-commerce Scams	11665	9783	$17.5M	$13.9M	$1,508
Job Scams	9043	9914	$156.2M	$135.7M	$17,281
Phishing Scams	8552	5938	$59.4M	$14.2M	$6,955
Investment Scams	6814	4030	$320.7M	$204.5M	$47,077
Fake Friend Call Scams	4179	6859	$13.6M	$23.1M	$3,263
Government Officials Impersonation Scams	1504	893	$151.3M	$92.5M	$100,622
Sexual Services Scams	1162	1141	$4.1M	$3.6M	$3,613
Loan Scams	1154	914	$6.0M	$6.1M	$5,212
Internet Love Scams	852	913	$27.6M	$39.8M	$32,470
Social Media Impersonation Scams	728	1570	$26.4M	$9.7M	$36,283
Top 10 scams	**45,653**	**41,955**	**$783.4M**	**$543.5M**	**$17,160**

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

Annex B

Small Number of Cases Involving Very High Losses

Other scam types such as malware-enabled scams, business email compromise scams and social media impersonation scams were noted to have also contributed to the sharp increase in total amounts lost, due to some cases involving very high losses.

a) While **malware-enabled scams** saw a decrease in number of cases by 84.8% to 289 cases in 2024, the total amount lost to this scam type increased by 278.6% to $129.1 million. **This was largely attributed to a single case that amounted to about $125.0 million losses in cryptocurrency**.

    - In this case of malware-enabled scam, the victim discovered unauthorised cryptocurrency transactions after clicking on fake interview meeting links and was asked to run a script on his laptop – the script was a malicious code that targeted cryptocurrency wallets.

b) Similarly, **business email compromise scams** saw a slight decrease in number of cases, by 1.1% to 368 cases in 2024, while the total amount lost to this scam type increased by 107.8% to $88.5 million. **This is largely attributed to a single case that amounted to $57.2 million in losses.**

    - In this case of business email compromise scam, the victim company fell prey to a scam variant involving business dealings. The company received an email purportedly from a known vendor informing on a change in bank account details for payment. They then made payment to the “updated” bank account. The victim company subsequently realised that they had been scammed when they received a late payment notice from the actual vendor.

c) The significant increase in total amount loss to **phishing scams**, by 318.4% to $59.4 million, is also **largely attributed to a single case that amounted to about $33.8 million losses in cryptocurrency**.

    - In this case of phishing scam, the victim chanced upon a phishing advertisement offering lucrative rewards while browsing on a legitimate cryptocurrency wallet application. The victim was redirected to a third-party site resembling the company behind the legitimate crypto wallet application, scanned a QR code and provided crypto wallet login credentials. The victim subsequently discovered unauthorised cryptocurrency transactions.

d) While **social media impersonation scam cases** decreased by 53.6% to 728 cases, the total amount lost increased by 172.0% to about $26.4 million in 2024.

This is largely attributed to a single case where about $21.7 million was lost in cryptocurrency.

- In this case of social media impersonation scam, the victim made cryptocurrency transfers under the impression that he was communicating with a known contact (e.g. company director) via Telegram.

It is estimated that the amount lost in the four scam cases involving very high losses mentioned above, accounted for 21.4% of the total scam losses in 2024.

Annex C

Backgrounder on Common or Notable Scam Variants

E-commerce Scams

- 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 22.4% of the total e-commerce scam cases in 2024, as compared to 11.7% in 2023. 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. In 2024, concert ticket scams have pivoted to take place on messaging platforms such as Telegram, where interventions and disruption efforts harder compared to traditional e-commerce marketplaces.

Job Scams

- Job scams recorded the second highest number of reported cases among all scam types in 2024, with 9,043 cases reported. The total amount lost to job scams in 2024 was also the second highest, with at least $156.2 million in losses.

- The majority of job scam victims were aged 30 to 49, making up 44.5% 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 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, Facebook, TikTok 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. 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 from the bank accounts, or when the scammers could no longer be contacted.

- In 2024, 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.

<u>Phishing Scams</u>

- Phishing scams recorded the third highest number of reported cases among all scam types in 2024. There were 8,552 phishing scam cases reported in 2024 and the total amount lost was at least $59.4 million.

- The majority of phishing scam victims were aged 30 to 49, comprising 42.2% of victims for this scam type. Facebook, Carousell and WhatsApp 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 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.

- 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 would encounter advertisements or sponsored posts on social media platforms such as Tik Tok, Facebook and Instagram on heavily discounted items ranging from homeware, personal accessories, electronics, food to cleaning supplies. These advertisements/posts offered enticing promotions/attractive deals to lure victims into clicking on to them. Victims would then be directed to external/third-party malicious websites where they were prompted to key in their bank card details and/or One-Time Passwords (OTPs)/perform digital authentication. Scammers would also 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 OTPs/perform digital authentication.

    - Victims would receive unsolicited phone or in-app calls allegedly from government officials such as the Singapore Police Force (SPF), Immigration & Checkpoints Authority (ICA), or 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, personal details, and/or OTPs/perform digital authentication.

    - Scammers would impersonate legitimate delivery companies and approach victims via text message (i.e. SMS, RCS, or iMessage) or email about a failed parcel delivery due to an incomplete addresses or that their parcels are currently held up at customs and require additional custom duties. Victims would then be instructed to click on the embedded link within the message content. Victims would then be directed to a phishing/spoofed delivery site which would prompt them to key in their debit/credit card details and OTPs/perform digital authentication.

- 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. In some cases which saw increased prevalence in 2024, phished card details were added to mobile wallets (i.e. Apple Pay, Google Pay, Samsung Pay), which would subsequently be used to conduct unauthorised transactions in stores. 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.

<u>Investment Scams</u>

- Victims of investment scams usually came across “investment opportunities” through recommendations from online friends or from their own internet searches. Some victims also received unsolicited messages from scammers offering “investment opportunities”. Once they were duped or had been enticed by the false testimonies, victims followed scammers’ instructions to transfer monies to specified bank accounts or cryptocurrency wallets or made payments via their bank cards for the purpose of investing. 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. “Investment” websites or applications displaying alleged growing “profits” earned by victims would also lead them into investing larger sums. 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 an approach which saw increased prevalence in 2024, victims were added into chatgroups or channels via messaging platforms such as WhatsApp and Telegram by scammers, for purported “investment opportunities”. In these chatgroups or channels, other “members” in the chatgroup would claim that they have profited by sharing screenshots of their “profits”, luring victims into believing that the investment was authentic and profitable. Tempted by the alleged “profits”, victims would contact the scammers and would be offered various investment plans. The scammers would ask for their personal information such as bank account number, name and phone numbers to join the “investment”. Victims would be instructed to transfer monies to specified PayNow numbers or bank accounts for the “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”. Scammers may also use “investment” websites or applications to display “profits” to reinforce the deceit.

Fake Friend Call Scams

- While fake friend call scams saw decreases in both number of cases and amounts lost in 2024, it remains among the top five scam types in terms of number of cases. The number of fake friend call scam cases decreased by 39.1% to 4,179 cases from 6,859 cases in 2023, and the total amount lost also decreased, by 41.1% to at least $13.6 million in 2024, from at least $23.1 million last year.

- The majority of fake friend call scam victims were aged 50 to 64, making up 35.7% of victims for this scam type.

- Fake friend call scams typically involve scammers contacting victims via phone calls or WhatsApp, and pretending to be their acquaintance. During the conversation, the scammers would claim that they had lost their mobile phone and changed phone number. After establishing rapport, the 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 contractors for renovation fees, pay for costs relating to the opening of new businesses, or pay vendors/suppliers. The victims would transfer money via PayNow to bank accounts belonging to unknown persons. They would discover that they had been scammed when they contacted their actual acquaintance and realised that they had neither changed their contact number nor contacted them.

Government Officials Impersonation Scams

- There were 1,504 government officials impersonation scam cases reported in 2024. The total amount lost to government officials impersonation scams in 2024 is the third highest, at least $151.3 million.

- The majority of government officials impersonation scam victims were aged 50 to 64, comprising 28.6% of victims for this scam type. Phone 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 such as 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 notable variants include the following:

- Impersonation of bank staff and local government officials through calls – Victims typically received unsolicited calls from scammers impersonating bank officers, who would seek verification on banking or financial transactions allegedly conducted by the victims. When victims denied 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". Scammers would instruct victims to transfer money to bank accounts also known as "safety accounts", supposedly designated by the government, purportedly for investigation purposes. This variant saw an increase of 87.8% to 1,151 cases in 2024, and 69.2% increase in amount lost to $107.4 million.

- 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 or bank officers, who would allege that victims had applied for credit cards, bank accounts or phone numbers that were eventually involved in criminal activities. In some cases, 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). Scammers would instruct victims to transfer money to "safety accounts" supposedly designated by China authorities, purportedly for investigation or bail purposes. This variant saw an increase of 26.1% to 353 cases in 2024 and 51.0% increase in amount lost to $43.8 million.