SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

POLICE NEWS RELEASE

ANNUAL CRIME BRIEF 2021

Our Streets Remain Safe but Scams are a Major Concern

Rise in scam cases drove overall crime rate higher

Singapore's streets remained safe in 2021, with a decease in physical crimes.[1]

2. However, a 52.9% increase in scam cases drove up the total number of reported crimes to 46,229 cases, from 37,273 cases in 2020. The Overall Crime Rate increased concomitantly, with 848 cases per 100,000 population in 2021, compared to 656 cases per 100,000 population in 2020.[2] Scammers have been constantly evolving their tactics and taking advantage of the COVID-19 situation to prey on the public's increase in online activities, and also their heightened sense of vulnerability and uncertainty.

3. Excluding scams and cybercrimes, the total number of reported crimes in 2021 decreased by 0.8% to 19,343 from 19,498 in 2020. In 2019, there were 23,980 reported cases of crimes excluding scams and cybercrimes.

Decrease in physical crimes and more crime-free days

4. There was a decrease in physical crimes in 2021. There were 250 days which were free from three confrontational crimes, namely snatch theft, robbery and housebreaking, an improvement of 48 days compared to 202 crime-free days in 2020. Of note, two out of the six crime classes that make up Overall Crime decreased significantly in 2021 compared to 2020, even with the Circuit Breaker in 2020. First, theft and related crimes decreased by 8.0% to 6,839 cases in 2021, from 7,437 cases in 2020. Second, housebreaking and related crimes decreased by 23.8% to 160 cases in 2021, from 210 cases in 2020. Both are a 37-year low.

5. The decline in physical crimes can be largely attributed to the Police and partners' continuous crime prevention efforts, Police presence on the ground and the use of technology to deter crime. Since the implementation of Police Cameras (PolCams) at all public housing blocks and multi-storey carparks in 2012, they have helped deter crimes such as housebreaking, motor vehicle theft and theft from motor vehicles. PolCams have also helped the Police to solve crimes, more than 6,000 cases

---

[1] Overall Crime excluding scams and cybercrimes.
[2] Overall Crime Rate refers to the Overall Crime per 100,000 population. It is computed by dividing the number of crime cases reported over the total Singapore population, and multiplied by 100,000.

to-date. More than 90,000 PolCams have been installed. The Police aim to have more than 200,000 PolCams installed islandwide by 2030.

Scam Situation

6. The total number of scam cases reported rose by 52.9% to 23,933 cases in 2021, from 15,651 cases in 2020. It made up 51.8% of Overall Crime in 2021, up from 42% in 2020.

7. The total amount cheated for the top ten scam types increased to $503.5 million in 2021, from $175.2 million in 2020. Please see **Annex A** for the statistics on the top ten scams.

Top scams of concern

8. Job scams, non-banking related phishing scams, e-commerce scams, investment scams, loan scams and banking related phishing scams remain of particular concern. They made up 80.4% of the top ten scam types reported in 2021. The total number of reported cases for these top six scam types rose by 99.3%, compared to 2020.

a) Job scams
- Job scams have become the top scam type, with the highest number of reported cases in 2021.
- The number of job scam cases jumped to 4,550 cases in 2021, from 132 cases in 2020.
- The total amount cheated increased to at least $91.0 million in 2021, from at least $217,000 in 2020.
- The largest sum cheated in a single case in 2021 was $4.3 million.
- Advertisements on various social media platforms (such as Facebook, Instagram, Telegram and TikTok), WhatsApp and Short Message Service (SMSes), and approaches made via dating platforms (such as Tantan and Facebook Dating) were common methods used by the scammers to reach out to the victims.

b) Non-banking related phishing scams
- The number of cases increased more than four-fold to 2,787 cases in 2021, from 644 cases in 2020.
- The total amount cheated jumped to at least $15.4 million in 2021, from at least $984,000 in 2020.
- The largest sum cheated in a single case in 2021 was $3.4 million.
- In the majority of these cases, the culprits used reasons such as checks on the delivery status of a parcel or refund for unauthorised transactions to persuade victims to provide their banking credentials or card details and one-time password (OTP).
- SMSes, calls and emails were the most common channels used by the scammers to approach the victims.

c) E-commerce scams
- The number of cases decreased by 18.8% to 2,729 cases in 2021, from 3,359 cases in the same period in 2020.

- The total amount cheated decreased to at least $5.9 million in 2021, from at least $7.1 million in 2020.
- The largest sum cheated in a single case in 2021 was $400,000.
- The most common platforms where these scams took place include Carousell, Facebook, and Shopee, while the common items involved in the transactions were electronic goods and gaming-related items (see **Annex B** for the breakdown of e-commerce scams on the various platforms).

d) Investment scams
- The number of investment scam cases more than doubled to 2,467 cases in 2021, from 1,096 cases in 2020.
- The total amount cheated increased to at least $190.2 million in 2021, from at least $68.8 million in 2020.
- The largest sum cheated in a single case in 2021 was $6.4 million.
- Common platforms used by scammers to communicate with victims included Facebook, Tinder, and Instagram.

e) Loan scams
- The number of loan scam cases increased by 14.9% to 2,273 cases in 2021, from 1,978 cases in 2020.
- The total amount cheated increased to at least $18.3 million in 2021, from at least $14.3 million in 2020.
- The largest sum cheated in a single case in 2021 was $361,000.
- Websites, SMSes, WhatsApp messages, and advertisements on social media or e-commerce sites were the more common channels used by the scammers to reach out to potential victims.

f) Banking related phishing scams
- The number of cases increased by 66.9% to 2,236 cases in 2021, from 1,340 cases in 2020.
- The total amount cheated more than tripled to at least $19.4 million in 2021, from at least $5.3 million in 2020.
- The largest sum cheated in a single case in 2021 was $1 million.
- In these cases, culprits impersonated banks or government officials. They approached victims via calls (phone call/in-app calls e.g. WhatsApp), and convinced the victims to provide bank card or account details and OTP, by pretending to assist the victims with issues concerning the victims' bank card or account. They also sent unsolicited SMSes claiming that there were issues with the victims' banking account, and the victims were asked to click on a link embedded in the text message to resolve the issue. Upon clicking on the link, the victims were redirected to fake bank websites and asked to key in their internet banking account login details. In some cases, the SMSes would state a phone number, belonging to the scammers, that the victims could call to seek help with their suspended bank card. Subsequently, victims found unauthorised transactions made to their bank account.
- Calls and SMSes were the most common channels used by the scammers to approach the victims.

9. Please see **Annex C** for the modus operandi of the top six scam types in 2021.

Police Efforts to Fight Scams

Anti-Scam Centre continues to disrupt scammers' operations

10. In March 2021, the Singapore Police Force (SPF) set up the Anti-Scam Division (ASD) to coordinate all of its anti-scam investigations and enforcement. The ASD investigates scam-related cases, focusing on detection, disruption as well as loss mitigation.

11. The Anti-Scam Centre (ASC), which is under the ambit of the ASD, uses technology to track scam trends and analyse crime data. In 2021, the ASC received more than 23,800 reports with losses amounting close to $520 million. In the same period, the ASC froze more than 12,600 bank accounts and recovered more than $102 million.

Strengthened enforcement against scam operations

12. The SPF continued to take tough anti-scam enforcement actions against local scammers and money mules. In 2021, the SPF conducted 26 islandwide anti-scam enforcement operations, leading to the investigation of more than 7,500 money mules and scammers.

13. Between September 2021 and November 2021, the SPF conducted three islandwide anti-scam enforcement operations targeting money mules linked to job scams. These led to the arrest of 135 individuals and investigation of 141 others for selling their bank accounts, or relinquishing their Singpass credentials to criminal syndicates to open bank accounts, to serve as conduits to receive funds from scam victims.

14. To disrupt scammers' operations to transfer money away from victims' accounts, the ASC works closely with the Monetary Authority of Singapore (MAS) and financial institutions to swiftly freeze bank accounts suspected to be involved in scams. In 2020, the ASC initiated Project FRONTIER (Fund Recovery Operations & Network Team, Inspiring Effective Resolutions). Under Project FRONTIER, once the Police are notified, most bank accounts suspected to be involved in scammers' operations can be swiftly frozen within a day, as opposed to the 14 to 60 working days that these processes used to take. From the initial 30 members, the ASC currently partners more than 60 institutions under Project FRONTIER.

15. To counter criminals who exploit fraudulently registered prepaid SIM cards as an anonymous channel of communications for illicit activities such as unlicensed moneylending, scams and vice, the SPF conducted simultaneous raids targeting 17 handphone shops in a nine-hour islandwide operation on 16 January 2022. Ten persons were arrested for their suspected involvement in fraudulently registering prepaid SIM cards using the particulars of unsuspecting customers or foreigners who have not entered or have left Singapore, and 24 others are assisting with investigations. These handphone retailers are suspected to have abused the computer systems holding registration information for prepaid SIM cards and selling them to customers who wanted to remain anonymous. The ASC has also worked with telecommunication companies and online marketplaces to terminate more than 3,300 mobile lines, report more than 17,300 WhatsApp lines, and remove more than 1,300 suspicious online monikers and advertisements involved in suspected scams.

16. The SPF also took to task money mules who had helped to facilitate the scams. The scammers commonly use bank accounts surrendered or operated by money mules to obscure their involvement and launder their criminal proceeds. In 2020, the Payment Services Act 2019 (PS Act) came into force, making this a specific offence. Prior to the operationalisation of the PS Act, money mules could only be prosecuted under the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (CDSA) for money laundering, which needed a much higher legal threshold. With the PS Act, money mules can now be charged with the offence of carrying on a business of providing payment services without a licence. On 10 January 2022, a man was sentenced to seven weeks' imprisonment and a fine of $645 for carrying on a business of providing a payment service without a licence under the PS Act. He had received funds in his bank accounts and made outward transfers to an overseas bank account. To-date, at least seven individuals have been convicted of carrying on a payment services business in Singapore without a licence. To further disrupt scammers' operations, Police are considering additional legislative levers to take even stronger and more effective action against money mules.

Leveraging technology to combat scams

17. The ASC launched Project COMBAT (Centralised Operational Messaging Bot, Addressing Threats) on 17 July 2021, to leverage technology to tackle the increase in scams. Through sense-making and collaboration with Police intelligence units and land division units, the ASC was able to detect many potential victims and alert them to the danger before they fell prey to the ongoing scam. The ASC conducted more than 6,900 successful interventions between May and December 2021.

18. One example is Project Awakenings, which the ASC launched on 3 December 2021, and which proactively engages potential victims on investment scams. Information is gleaned through crowdsourcing within the Police: The ASC has set up a framework that gets Police officers to submit to the ASC, screenshots of suspicious WhatsApp groups promoting unregulated investment products, gleaned from their own contacts or during interactions with the public. Using Optical Character Recognition (OCR) technology, ASC has automated the capturing of the local handphone numbers of participants in the WhatsApp groups, and then sends out targeted advisories to these potential victims via SMS (SG-Mail) with the use of Robotic Process Automation. As of end December 2021, more than 1,300 potential victims of investment scams had received the advisory.

ScamShield mobile application

19. The ScamShield mobile app, jointly developed by the National Crime Prevention Council (NCPC) and the Open Government Products team from the Government Technology Agency, identifies and filters out scam messages using artificial intelligence. It also blocks calls from phone numbers that were used in other scam cases or reported by ScamShield users. These two functions reduce opportunities for scammers to reach out to intended victims.

20. The app was launched on 20 November 2020. It is currently available for iPhone users, and an Android version will be rolled out in the first half of 2022.

21. Since its launch, ScamShield has been downloaded more than 257,000 times. More than 3.7 million SMSes and calls have been picked up as potential scams, and

more than 15,500 phone numbers have been blocked from making calls to users of the application.[3]

22. Please see **Annex D** for comments from the Director of the Commercial Affairs Department.

Collaboration with foreign law enforcement agencies

23. On the international front, the Police work closely with foreign counterparts and partners such as the Hong Kong Police Force, the Royal Malaysia Police, and Interpol, to exchange information and conduct joint investigations and operations against transnational scams.

24. Through this close collaboration, the Police and overseas law enforcement agencies successfully took down 16 scam syndicates comprising nine job scam syndicates, four China/Government Officials impersonation scam syndicates and three internet love scam syndicates in 2021, leading to the arrest of more than 230 persons who were responsible for more than 1,350 cases.

Continued public education efforts to raise awareness on scams

25. To educate the public, the Police and NCPC proactively disseminate information and advisories on scams, and highlight successful prosecutions on a regular basis. For example, NCPC's commissioned programme 'CrimeWatch' features a regular 'Scam Alert' segment which highlights topical scams and provides prevention tips to viewers. In addition, NCPC regularly shares scam prevention tips and advisories with the public through various social media and messaging platforms. It has also commissioned various media content pieces to share crime prevention tips with members of the public, and in particular to educate them on scam signs to look out for. The Police also collaborate with other partners to raise awareness of scams.

26. SPF formalised an e-Shoppers on Watch interest group under the Cyber category of the Community Watch Scheme (CWS) to share the latest crime concerns and scam advisories. Members are encouraged to share such useful information with their loved ones to prevent them from being victims of crime.

27. The NCPC and SPF, in collaboration with SGAG, also rolled out an anti-scam jingle via social media platforms. The jingle references the style of Korean popular music (K-pop) videos. Its chorus uses the catch phrase of "Spot the Signs. Stop the Crimes.", which is the tagline for the current Anti-Scam Campaign. The lyrics describe a few scam tactics typically used by scammers such as requests for OTPs.

Introduction of E-Commerce Transaction Safety Ratings

28. E-commerce scams continue to be one of the top scam types in Singapore. As such, the Inter-Ministry Committee on Scams (IMCS) will be introducing the E-Commerce Marketplace Transaction Safety Ratings (TSR) later this year. The TSR will provide an indication of the extent to which different e-commerce marketplaces have in place anti-scam measures that the Ministry of Home Affairs (MHA) assesses to be most critical in combating e-commerce scams.

29. The TSR will serve to:

---

[3] Figures updated as of 31 January 2022.

a. Create awareness on features that keep e-commerce transactions safe, and how to use these features;
b. Allow consumers to make an informed choice on which e-commerce marketplace to use for their transactions, based on the availability of safety features on the marketplace; and
c. Raise consumer vigilance, and encourage the use of safety features and good practices when transacting online.

30. The first TSR Report and more details on this initiative will be released later this year.

Public vigilance essential to combatting scams

31. The prevalence of scams is high in Singapore, as in many other parts of the world. At least 90% of scams in Singapore originate from overseas and these scammers are syndicated, well-resourced and technologically sophisticated. Such cases are difficult to investigate and prosecute, as our efforts will be dependent on the level of cooperation from overseas law enforcement agencies, and their ability to track down the scammers operating in their jurisdiction. Where monies have already been moved outside Singapore, recovery is very difficult.

32. Given the rate at which new scam variants are surfacing, a discerning and well-informed public is the best defence.

33. The Police will continue to work with the NCPC and other stakeholders to educate the public about scams. We will focus our efforts in the online realm, where most of the scams are taking place.

34. Members of the public are advised to keep themselves informed of the latest scam variant. They can visit the website www.scamalert.sg to learn about the various types of scam and steps they can take to avoid falling prey.

35. Please see Annex E for comments from the Chairman of NCPC.

Rise in Voyeurism Cases

36. Voyeurism cases increased to 467 in 2021, from 394 cases in 2020. A lower number of voyeurism cases was recorded in 2020 likely because of the lower ridership on public transport, lower footfall at shopping malls, and the closure of public entertainment outlets during the Circuit Breaker.

37. The top three locations, where about 67.2% of voyeurism cases occurred were:

a) in residential premises – there were 179 such cases reported in 2021, as compared to 105 cases reported in 2020;
b) on the public transport system – there were 79 such cases reported in 2021, as compared to 68 cases reported in 2020; and
c) in shopping complexes – there were 56 such cases reported in 2021, as compared to 58 cases reported in 2020.

38. Members of the public are reminded to stay vigilant against voyeurism by being aware of their surroundings. They are also advised to make a police report as soon as possible if they are a victim of voyeurism or have witnessed the crime being committed.

Reporting such crimes early is crucial in helping the Police identify and arrest the perpetrators.

Rise in Outrage of Modesty (OM) Cases

39. OM cases increased to 1,474 cases in 2021, from 1,321 cases in 2020. This increase was partly due to a lower number of OM cases recorded in 2020 because of the Circuit Breaker. In 2019, there were 1,605 OM cases. OM cases accounted for 46.3% of all sexual crime cases reported in 2021.

40. Of the 1,474 OM cases in 2021, 915 cases involved culprits known to the victim.

41. The number of OM cases occuring within the public transport system, including at public transportation nodes and on public transport, remains a concern. There were 147 OM cases in 2021 involving culprits unknown to the victim and which occurred on the public transport system, compared to 145 the previous year.

42. The Police continue to work closely with public transport operators and partners, including the NCPC, to reach out to commuters to raise awareness. For example, posters on voyeurism and OM are prominently displayed on MRT trains, and at train stations and bus interchanges. Public education videos on OM are screened at MRT stations. In September 2021, advisories on OM were distributed to commuters who were registered on various transport-related mobile apps such as the Land Transport Authority (LTA) MyTransport app, SMRTConnect app, and SBS Transit app. The Police also utilise targeted advertising through multiple platforms including online channels such as social media platforms, out-of-home spaces, and advertisements on TV and radio. These advisories and videos educate the public on what they can do when they encounter such crimes, and remind them to stay vigilant and report the matter to the Police if they encounter anything suspicious.

43. Riders on Watch (ROW), a programme that has been subsumed under the CWS, was introduced in 2019 to encourage commuters to be vigilant to crime and security concerns while travelling on the public transport network. ROW taps on commuters to act as additional ‘eyes and ears’ on public transport for the Police, with volunteers keeping watch for suspicious persons or activities, and providing valuable information to the Police. These volunteers also receive regular crime advisories affecting the public transport system.

Cyber Extortion Cases are a Concern

44. The number of cyber extortion cases increased to 421 cases in 2021, from 245 cases in 2020. In these cases, criminals typically befriend victims online and subsequently coax them into performing compromising or indecent acts in front of a camera. Thereafter, the criminals would use the video footage or images to extort money or online credits from these victims. In some cases, victims were asked to visit a link or to download an app that may result in granting the criminals access to the victims’ contact data, which will then be used to extort the victims. The total amount lost by victims of cyber extortion cases was at least $1.3 million. The most common social media platforms where these cases took place were Facebook, Instagram and Tinder.

45. The Police have been working with the grassroots community to reach out to members of the public, to alert them to the threat of cyber extortion and share crime prevention measures.

Business Operators and the Community Play a Key Role in Fighting Crime

46. Criminals, including scammers, remain a threat to public safety and security. The ongoing COVID-19 situation provides opportunities for them to exploit the public's fear and sense of uncertainty, and to develop new schemes and target new victims. This is evident from the significant increase in online scam cases reported in 2021.

47. Everyone has a part to play in keeping Singapore safe and secure, especially during these uncertain times. Business operators such as banks, online marketplaces and telcos have a responsibility to prevent, deter and detect crimes committed through their platforms. Putting in place anti-scam measures and precautions against crimes will also help business operators keep their customers safe.

48. To recognise the community and business operators for their support in helping to keep Singapore safe and secure, the Police presented 80 Public Spiritedness Awards and 131 Community Partnership Awards in 2021. We encourage the community to continue to support us in the fight against crime.

49. Family members and friends also play an important part. They can prevent someone they know from falling victim, by being aware of the threats and cautioning their loved ones about them. Members of the public should stay vigilant and report any crime-related information to the Police.

50. In December 2021, the Police launched the CWS, which integrates the various watch groups, including the Neighbourhood Watch Zone (NWZ), Vehicles on Watch and ROW, under one umbrella scheme. Anchored on five categories, with various groups created under each category to cater to different interests, CWS harnesses the community spirit of these interest groups to build a larger community regardless of geographic boundaries, where everyone can be vigilant while engaged in their areas of interest. CWS members can sign up for one or more of the interest groups. Upon doing so, they will receive regular updates, including crime-related advisories, as well as opportunities to participate in related activities, training, and workshops. In turn, CWS members are encouraged to actively share crime information from the Police with their loved ones and prevent them from being victims of crime, to be vigilant, and to share relevant crime information they come across with SPF.

51. We encourage more members of the public to join the CWS, and to work with us to keep Singapore safe and secure for everyone.

52. Please see Annex F for comments from the Director of Operations Department.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
16 FEBRUARY 2022

ANNEX A

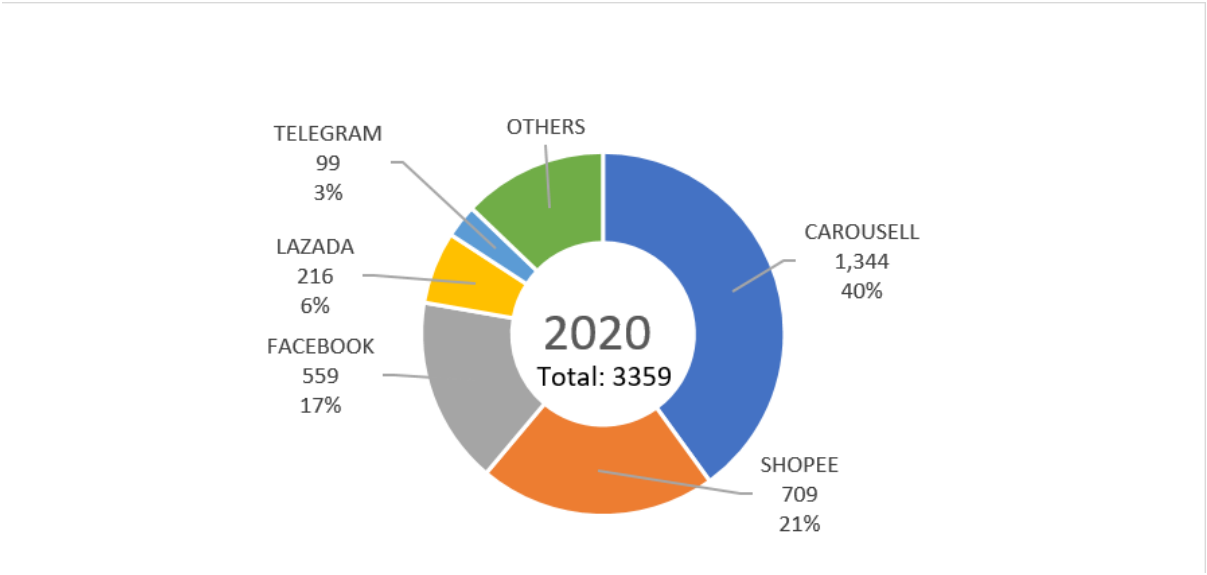
TOP TEN SCAM TYPES IN SINGAPORE IN 2021

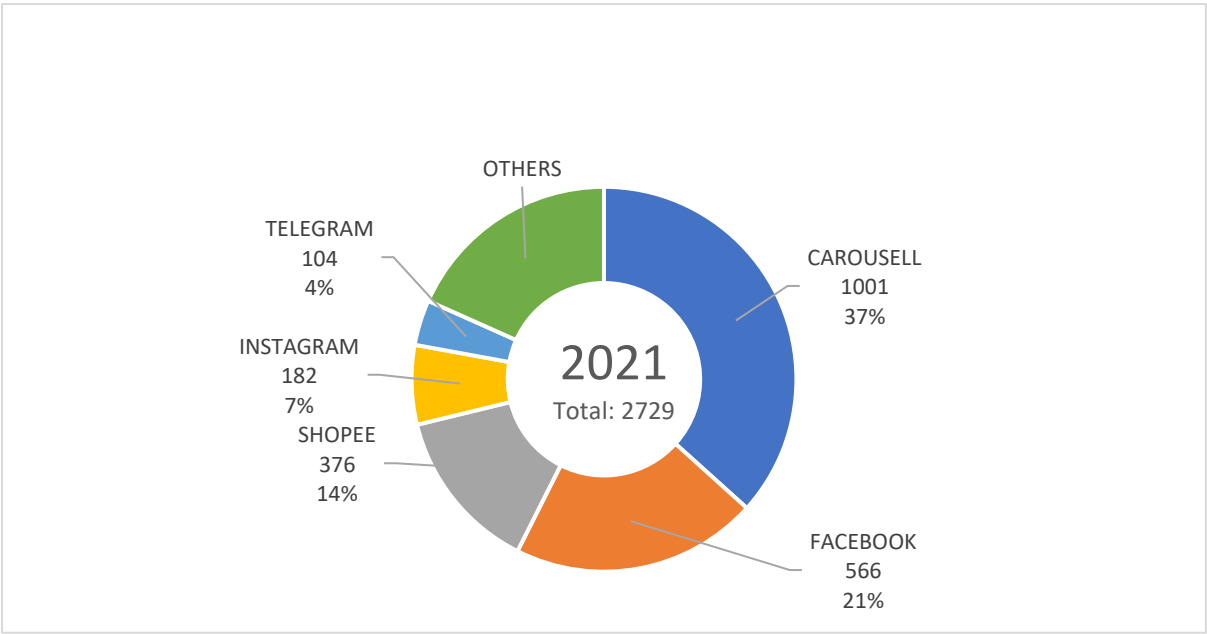
	Cases Reported		Amount Cheated		
	2021	Change from 2020	2021	Change from 2020	Largest sum cheated
Job Scams	4,550	+4,418	$91.0m	+$90.8m	$4.3m
Non-Banking Related Phishing Scams	2,787	+2,143	$15.4m	+$14.4m	$3.4m
E-Commerce Scams	2,729	-630	$5.9m	-$1.2m	$400k
Investment Scams	2,467	+1,371	$190.2m	+$121.4m	$6.4m
Loan Scams	2,273	+295	$18.3m	+$4.0m	$361k
Banking Related Phishing Scams	2,236	+896	$19.4m	+$14.1m	$1.0m
Social Media Impersonation Scams	1,614	-1,305	$5.5m	+$50k	$1.0m
Internet Love Scams	1,094	+271	$46.6m	+$13.4m	$3.0m
China Officials Impersonation Scams	750	+308	$106.3m	+$66.7m	$6.2m
Fake Friend Call Scams	686	+686	$4.5m	+$4.5m	$616k
Total	**21,186**	**+8,453**	**$503.5m**[#]	**+$328.3m**	

[#] *The sum of the amount lost will not tally due to rounding.*

ANNEX B

TOP FIVE DIGITAL PLATFORMS USED IN E-COMMERCE SCAMS





ANNEX C

MODUS OPERANDI FOR THE TOP SIX SCAM TYPES IN 2021

TOP SIX SCAM TYPES	MODUS OPERANDI
Job Scam	The Police have observed four variants of jobs scams: i. In the first variant, victims were told to download fake mobile applications to grab the jobs through the application. Thereafter, they would be instructed to top-up funds into their account on the applications by either transferring the money to bank accounts provided, or converting the amount into cryptocurrency and transferring them into wallets provided by the scammer. As scammers would have allegedly promised victims their commission after a certain number of tasks have been completed, the amount would then be reflected in their mobile application accounts. However, the victims would later realise that they have been scammed when they were unable to withdraw the money from these accounts. ii. In the second variant, victims would receive a warning letter via WhatsApp and be pressured into making further fund transfers to bank accounts or cryptocurrency wallets provided if they have chosen to discontinue with these jobs. The letter would indicate that their mobile application accounts would be frozen and legal actions could be taken against them if they were to discontinue with the 'job'. The scammers have also included the emblems of SPF, Singapore's Coat of Arms as well as the Supreme Court on the warning letters issued to victims to enhance the credibility of their ruse. Victims would eventually realise that they have been scammed when they did not receive their commission after completing the tasks given to them by the scammers. iii. In the third variant, the victims received unsolicited text messages, Whatsapp messages, Facebook or Instagram posts, or came across advertisements online promoting highly paid part-time affiliate marketing related jobs. The scammers would offer fake online jobs which required the victims to complete easy tasks such as following social media accounts and liking social media posts to boost its viewership. In order to perform the job and earn their commission, the victims would be directed to sign up for free membership accounts on websites and mobile applications provided by the scammers. iv. In the fourth variant, the scammers would befriend victims on messaging applications such as MiChat and WeChat. These scammers would then introduce victims to purported job offers

	that would allow them to earn commission through the buying and selling of movie tickets involving various companies, such as Filmgo Production and Filmgo Digital etc. Victims would be directed to sign up for accounts on the "Filmgo" websites provided by the scammers. These websites would also offer mobile applications for victims to download and use its services conveniently. Victims would be required to top-up their "Filmgo" accounts in order to buy and sell movie tickets and earn commissions, and the scammers would provide victims with bank accounts belonging to unknown individuals for the payment to be made. Most of the time, the victims would be convinced that their work was legitimate as their "Filmgo" account indicated the commissions they received after completing the jobs. However, victims would eventually discover that they had been scammed when they were unable to withdraw the money from their "Filmgo" accounts.
Non-banking related phishing scams	The Police have observed two variants of non-banking related phishing scams: i. In the first variant, victims of such phishing scams would receive phone calls from scammers impersonating staff from e-commerce marketplaces. The scammers would claim that there were issues with the victims' accounts or payment discrepancies detected for victims' purchases. Under the pretext of assisting to rectify the issue, the victims would be tricked into providing their credit/debit card details and OTPs. Victims would only realise that they have been scammed when they discover unauthorised transactions made using their credit or debit card. ii. In the second variant, victims would receive emails or text messages from scammers impersonating entities that are known or trusted, such as banks, government agencies, trade unions, or companies such as SingPost, Grab or Netflix. These emails and text messages would make fake offers or claims in order to trick recipients into clicking on a phishing URL link. These fake offers or claims include outstanding payment for parcel delivery, disruptions to services or subscriptions, refunds, or promotions. Upon clicking on the phishing URL links, victims would be redirected to fraudulent websites where they would be tricked into providing their credit/debit card details and OTPs. Victims would only realise that they have been scammed when they discovered unauthorised transactions made using their credit/debit card.
E-commerce Scam	E-commerce scams involve a few variants, the most typical of which would involve culprits posing online as sellers of items. They cheat victims by failing to deliver the goods purchased after victims had paid for them. Instead of using the buyer protection in-built payment options on the E-commerce platforms, victims would be directed by the scammers to make advance payment or direct bank transfers before delivering the goods.
Investment Scam	In the majority of investment scams, the scammers would claim to be financial professionals and cultivate victims on online platforms. Once lured, the victims would be introduced by the scammers to investment websites or mobile applications where they would be enticed to invest

	and asked to transfer money to unknown bank accounts. Victims would also be asked to pay administrative fees, security fees or taxes, in order to reap profits. In many instances, victims would earn a profit from the investment at the initial stage, leading them to believe that the investment was legitimate and lucrative. Once larger amounts of monies were deposited into the designated bank accounts or when the victims realised they were unable to withdraw their money, the scammers would become uncontactable.
Loan Scam	In the majority of these cases, the victims came across loan offers or advertisements that were supposedly from licensed moneylenders or banks and required victims to provide their personal information to obtain the loan. Victims would also be asked to pay a small percentage of the loan amount as administrative fees and once the money had been transferred to the scammers, the scammers would become uncontactable. In some cases, the scammers would also ask the victims to transfer more funds for various fees, but eventually, no loan was disbursed to the victims.
Banking related phishing scams	Culprits would impersonate legitimate banks e.g. DBS/POSB or government officials such as SPF and MOM. Culprits would approach victims via calls (phone call/in-app calls e.g. WhatsApp), where they convince victims to provide their bank card /account details and OTPs by pretending to assist them with issues concerning their bank card / account. Culprits would also send unsolicited SMSes claiming that there were issues with the victims' banking accounts, and the victims would be asked to click on a link to resolve the issue. Upon clicking on the links embedded in the text messages, victims would be redirected to fake bank websites and asked to key in their iBanking account login details. In some cases, the SMSes would state a phone number, belonging to the scammers, that the victims could call back to seek help with their suspended bank card. Subsequently, victims would discover unauthorised transactions made to their bank accounts after providing their banking credentials and/or OTPs.

ANNEX D

Quote by Director of Commercial Affairs Department

Scams continue to increase, and scammers are constantly finding new ways to prey on victims' vulnerabilities. Many scams involve scammers who operate from outside of Singapore, using the internet to dupe their victims from afar. They use local money mules or take advantage of the victim's internet banking facilities to move the criminal proceeds out of Singapore, making recovery very difficult.

In response to this, the Anti-Scam Division was formed in March 2021 to ensure efficient enforcement coordination and swift information sharing to enhance the scam-fighting efforts of the Singapore Police Force. Since the formation of the Anti-Scam Division, the Singapore Police Force has successfully busted 16 transnational syndicates together with our foreign counterparts, leading to the arrest of more than 200 syndicate members.

Our Anti-Scam Centre has also seen an exponential expansion of its partnership network. Our partnership with over 30 financial institutions has proved instrumental in interdicting scam proceeds. 2021 saw the Anti-Scam Centre recovering scam proceeds of over S$102 million, almost twice the amount recovered in 2020. Our Anti-Scam Centre also proactively screens police reports for online monikers, URLs and advertisements linked to scammers' activities, and work with the relevant commercial entities (e.g. financial institutions, telcos, and online marketplaces) to disrupt the scammers' operations.

Whilst the Police will endeavour to safeguard the public from crime, combatting scams is a community effort, and the best defence against scams is an alert and discerning public. We will continue to curtail scammers' activities with the support of our stakeholders in the public and private sectors to achieve our vision of a Scam-Smart nation.

– Mr. David Chew
Director of Commercial Affairs Department

ANNEX E

Quote by Chairman, National Crime Prevention Council

With the number of scam cases on the rise, NCPC has redoubled its efforts in educating the public on scams. We will continue to leverage new technology and new content formats to reach out to the public in order to educate and protect them against scams. While tactics may change and get more sophisticated, the signs do not. Scammers are always out to get our personal and bank details or OTPs or money. They usually contact you from overseas via numbers with a '+' prefix. So, remember to spot these common scam signs in order not to become the next victim.

Vigilance still plays a critical role in scam prevention: All it takes is a few minutes of your time to look at the suspicious requests carefully and seek verification first before handing over any information and money. It is time well-spent to prevent yourself from experiencing the heartaches and monetary losses should you become a scam victim. Share these tips with your loved ones so that they are aware too!

I urge everyone to continue to stay alert and keep yourselves updated on the latest scams. I strongly believe that we can eventually win this fight against scams.

- Mr. Gerald Singham
Chairman, National Crime Prevention Council

ANNEX F

Quote by Director of Operations Department

The Police continue to leverage technology such as Police Cameras (PolCams) to deter and solve crimes. This has been effective as we see a sustained decrease in some types of physical crime and an increase in the number of crime-free days for snatch theft, robbery and housebreaking.

However, the rise in online scam cases is a concern. Criminals continue to develop new tactics to prey on vulnerable and unsuspecting victims, taking advantage of the COVID-19 situation and the prevalence of online banking, social media platforms and e-commerce sites to perpetrate their illegal activities.

The Police will continue to monitor the situation closely and work with our partners, the community and business stakeholders to fight crime. However, it is also crucial for the public to remain vigilant and stay updated on the latest *modus operandi* of scammers so that we can protect ourselves and our loved ones from becoming a victim of crime.

Fighting scams is a community effort and a discerning public remains the first line of defence to guard against rapidly evolving scam types. Let us stay informed, be vigilant and do our part in the fight against crime.

– Senior Assistant Commissioner of Police Lian Ghim Hua
Director of Operations Department