

POLICE NEWS RELEASE

MID-YEAR CRIME STATISTICS 2022

Overall Crime Situation for January to June 2022

Rise in Scam Cases Drove Overall Crime Higher

Scams continued to be the main driver of crime in the first half of 2022. From January 2022 to June 2022, an increase in scams to 14,349 cases drove up the total number of reported crimes to 25,593 cases, from 18,725 cases in the same period in 2021. Scammers have been constantly evolving their tactics, and facilitated by the increase in online activities.

2. The total number of physical crimes¹ in the first half of the year was 9,825 cases, up from 9,748 cases in the same period in 2021. However, this remains lower than the pre-COVID-19 figure of 13,015 reported in the same period in 2019.

Housebreaking and Robbery Continue to Decline

3. Housebreaking and related crimes decreased to 77 cases in the first half of 2022, from 88 cases in the same period last year. The number of cases of robbery decreased to seven in the first half of 2022, from 16 cases in the same period last year. The first half of 2022 recorded the lowest number of cases of housebreaking and robbery in the past 10 years.

Scam Situation

4. The total number of scam cases reported rose to 14,349 in the first half of 2022, from 7,746 cases in the same period last year.

5. The total amount cheated for the top ten scam types increased to \$227.8 million in the first half of 2022, from \$142.5 million in the same period last year. Please see <u>Annex A</u> for the statistics on the top ten scams.

Top Scams of Concern

¹ Overall Crime excluding scams and cybercrimes.

6. Job scams, phishing scams, e-commerce scams and investment scams remain of particular concern, and made up 74.5% of the top ten scam types reported in the first half of 2022.

- a) <u>Job scams</u>
- Job scams recorded the highest number of reported cases amongst all scam types in the first half of 2022. There were 3,573 cases reported, and the total amount cheated was \$58.5 million. The job scams generally offered attractive "commissions" for relatively simple tasks, but required the victims to provide their own funds. Victims would provide more and more funds to earn more "commission", but would eventually end up losing their money when they were unable to withdraw their funds.
- In most job scams, victims would come across online advertisements or receive unsolicited messages over chat applications such as Telegram and WhatsApp from unknown numbers, which offer part-time jobs with high salaries that can be performed from home. The message would also include a WhatsApp number as a point of contact for interested victims to sign up for the job by creating an account. A common variant of the scam entails the victim being asked to help e-commerce platform merchants improve their sales by making advance purchases. The scammer would assure the victims that their money would eventually be refunded, and a commission would be paid to the victims. The scammers would then provide an e-commerce platform item link to the victims and instruct them to provide a screenshot of the item in their shopping cart. Thereafter, the victims would be instructed to make payment for the item by transferring the money to a bank account number provided by the scammer. This process would be repeated several times, beginning with low-cost items before progressing to more expensive items. The scammers would initially refund the victims the cost of the item and the commission, but would later claim to have encountered issues with the refund and would stop paying the victims.
- In other variants, victims who contacted the number provided would be instructed by the scammers to complete tasks online, such as liking social media posts, or reviewing hotels and restaurants on a website, for a commission. The scammers would then provide the victims with a website to perform the tasks and would change the URL of the website frequently. The victims would also be told that they needed to top up their accounts with money to begin the tasks. After receiving an initial small payout for completing a certain number of tasks, victims would be told by the scammers to 'recharge' their job accounts by transferring money to various bank accounts, before more tasks could be performed. Victims would

realise that they had been scammed when they were unable to withdraw the money in their job accounts, and the scammers became uncontactable.

- In a Ponzi-like job scam variant, victims would be asked to purchase expensive memberships before they could take part in unrealistically lucrative job tasks. Victims would often do so until the sums became extremely high, and they no longer wished to continue. However, they would be told that they can only get back all their money when they finish all the tasks. Often, this would be when victims realise that they had been scammed.
- Advertisements on messaging applications such as WhatsApp and Telegram were common methods used by the scammers to reach out to the victims.
- b) Phishing scams
- Phishing scams recorded the second highest number of reported cases amongst all scam types in the first half of 2022. There were 2,301 cases reported and the total amount cheated was \$7.8 million.
- In banking-related phishing scams, culprits impersonated bank or government officials. They approached victims via calls (phone call/in-app calls e.g. WhatsApp), and convinced them to provide bank card or account details and OTPs, by pretending to assist 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 from their bank account.
- Calls and SMSes were the most common channels used by the scammers to approach the victims.
- In non-banking related phishing scams, 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 discover unauthorised transactions made using their credit/debit card.

- In another variant, the scammers would typically approach victims on Carousell and express interest in purchasing items that victims are selling. The scammers would request to make payment via CarouPay to the victims' PayNow account. Thereafter, the victims would receive an email purportedly sent from Carousell, indicating that the payment had been made. This phishing email would then instruct victims to provide their internet banking account login details via a phishing link or phishing PayNow QR codes provided with the email to receive payments. Upon clicking these links or scanning the QR codes, victims would be redirected to spoofed bank websites, where they were tricked into providing their banking details and OTPs in order to receive the payments. Victims would only realise that they have been scammed when they discover unauthorised transactions made from their bank account.
- SMSes and Carousell in-app messaging were the most common channels used by the scammers to approach the victims.
- c) E-commerce scams
- E-commerce scams generally involve the sale of goods online without delivering the items after payment is made.
- There were 2,267 e-commerce scams reported in the first half of 2022 and the total amount cheated was \$8.3 million.
- The increase in e-commerce scams is largely due to rental scams involving fake property listings, which made up 29.6% of e-commerce scams. Members of the public are advised not to make any payment before viewing the property and to verify the legitimacy of a listing by checking the contact number against the Council for Estate Agencies' website.
- In the majority of e-commerce scams, the scammers would post products for sale at a lower price as compared to the prevailing retail value. Enticed by the pricing, victims would then pay a deposit via bank transfer as required for the purchase of the products, which were not delivered.
- The most common platforms used by scammers to communicate with victims include Carousell, Facebook and WhatsApp / Telegram, while the most common items involved in the transactions were house / room rental,

electronic goods (e.g. mobile phones, earbuds / earpieces and televisions) and miscellaneous items such as collectibles, trading cards and graphics cards.

d) Investment scams

- There were 1,683 investment scams reported in the first half of 2022 and the total amount cheated was \$108.8 million.
- 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 had been transferred to the scammers, victims found that they were not able to cash out the earnings and the scammers would become uncontactable.
- Instagram, Facebook and Telegram were the most common platforms used by the scammers to approach the victims.

Police Efforts to Fight Scams

Enforcement

a) Formation of Anti-Scam Command

7. To achieve greater synergy between various scam-fighting units, the Commercial Affairs Department (CAD) operationalised the Anti-Scam Command (ASCom) on 22 March 2022. The newly established Command comprising the Anti-Scam Centre (ASC) and three Anti-Scam Investigation Branches, provides oversight and policy guidance for the Scam Strike Teams (SSTs) situated within the seven Police Land Divisions.

8. The ASCom consolidates expertise in combatting scams, and enhances the management of scam-related strategies and activities across the areas of investigation, intelligence, scam intervention, enforcement policy, and stakeholder engagement. Since its formation, ASCom has been working closely with the SSTs to tackle and solve syndicated and transnational scam cases through joint investigations and operations.

b) Anti-Scam Centre (ASC) Continues to Disrupt Scammers' Operations

9. In the first half of 2022, the ASC received more than 13,400 reports on scams. Acting on these reports, the ASC froze more than 7,800 bank accounts and recovered close to \$80 million, which was about 31.4% of the total amount scammed.

10. The ASC also works closely with local telecommunication companies to terminate mobile lines which are found to have been used for scams, as well as with social media platforms and online marketplaces to remove suspicious accounts and advertisements. From January to June 2022, over 1,600 such local mobile lines were terminated, and more than 2,500 suspicious online monikers or advertisements were removed. During the same period, the ASC also submitted more than 13,200 WhatsApp accounts which were believed to be used in scams, for review and removal.

11. The ASC and the Monetary Authority of Singapore are working with the banks to co-locate their staff at the ASC, to enhance real-time coordination with the Police in investigative efforts, tracing the flow of funds, and freezing bank accounts suspected to be involved in scammers' operations.

c) Strengthened Enforcement against Scam Operations

12. The Police continue to take tough anti-scam enforcement actions against local scammers and money mules. In the first half of 2022, the Police conducted 12 islandwide anti-scam enforcement operations, leading to the investigation of more than 3,400 money mules and scammers.

13. In March 2022, the Police conducted islandwide anti-scam enforcement operations targeting investment and job scams, as well as those who sold their Singpass account to fraudsters. These led to the arrest of 35 individuals and investigations into 255 others for relinquishing their Singpass credentials to criminal syndicates to register businesses and open bank accounts, or crypto-exchange accounts to serve as conduits to receive funds from scam victims. In some instances, the Singpass details were also misused by scammers to subscribe to new mobile lines to communicate with victims.

d) Collaboration with Foreign Law Enforcement Agencies

14. As scams still predominantly originate from overseas, the Police have stepped up collaboration with foreign law enforcement agencies. In the first half of 2022, a total of seven joint operations were conducted with overseas law enforcement agencies such as the Royal Malaysia Police (RMP), leading to the arrest of 39 syndicated members overseas.

15. In January 2022, the Commercial Crime Investigation Department (CCID) of the Royal Malaysia Police (RMP) raided a call centre in Kuala Lumpur and arrested 23 members of a job scam syndicate. The group had been targeting victims in Singapore and other countries. Working on information uncovered during the raid, officers from the ASCom and Police Land Divisions conducted an islandwide operation

and investigated 10 individuals for their suspected involvement in assisting the scam syndicate to launder about \$319,000 of scam proceeds in Singapore.

16. In April 2022, the ASCom and RMP CCID conducted a joint operation against a love scam syndicate operating in Malaysia. A team comprising ASCom and CCID officers raided two locations in Kuala Lumpur and arrested six Nigerian individuals who had been targeting Singapore victims.

Engagement

a) Proactive Intervention for Scam Victims

17. The ASC routinely carries out physical interventions with potential victims of scams. A total of 240 interventions have been conducted, preventing transfers of more than \$41 million which would have been otherwise lost to scammers. Through fund tracing and analysis of money mule accounts, unsuspecting victims of scam arrangments, who may still be transferring money to scammers, are identified. ASC officers, together with officers from Police Land Divisions and banks, work together to engage such unsuspecting victims. The victims would be informed that that they could have fallen prey to scams and are advised to stop any further monetary transfers. Many of the victims were completely unaware that they had been scammed, prior to Police's engagement.

18. During an operation in March 2022, a total of 264 potential victims were engaged, of whom 157 were eventually convinced that they had been scammed and lodged police reports.

b) ScamShield Mobile Application

19. The ScamShield mobile application (app) is jointly developed by the National Crime Prevention Council (NCPC) and Open Government Products, Government Technology Agency (OGP/GovTech). The app identifies and filters out scam messages and blocks calls from phone numbers that are verified as scam-related. These two features reduce the opportunities for scammers to reach out to intended victims. In addition, the app enables users to report scam messages and receive alerts on trending scams.

20. The ScamShield iOS app was launched on 20 November 2020. Since its launch, the app has been downloaded by more than 300,500 iOS users. Since inception, more than 5.1 million SMSes have been reported, and over 24,500 phone

numbers believed to be used for scam calls have been blocked.² The ScamShield Android app will be made available next month.

Education

a) Continued Public Education Efforts against Scams

21. The prevalence of scams continues to be high in Singapore. At least 90% of scams in Singapore originate from overseas. These scammers are typically part of organised criminal groups, and run sophisticated transnational operations which are not easy to detect or dismantle. These scammers are also well-resourced, and adept at using technology to cover their tracks. Such cases are difficult to investigate and prosecute, as tracing the scammers depends on cooperation from overseas law enforcement agencies, and their ability to track down the scammers operating in their jurisdiction. Where money has already been moved outside Singapore, recovery is very difficult. Hence, it is of utmost importance that should any member of the public suspect that they have been scammed and their bank accounts compromised, they should immediately notify their bank and lodge a police report online via www.police.gov.sg/iwitness, or at any neighbourhood police centre.

22. A discerning and well-informed public is the best defence against scams, especially given the increase in scam variants. To this end, the SPF continues to work closely with NCPC to conduct public education on scams, particularly online, where most scams are taking place.

23. In collaboration with the Association of Banks in Singapore (ABS), the Police, and MoneySense, NCPC rolled out a revamped bank quiz (Annex B) at <u>www.scamalert.sg/scambusterbankquiz</u> that seeks to educate retail bank customers on various scams such as bank-phishing, investment and job scams. This year's quiz features more interactive elements and actual scam examples to educate bank customers on how to spot scams and red flags, and what to do upon receiving such scam messages. Besides the NCPC website, bank customers will also be able to access the quiz through their mobile banking apps and various social media platforms. The first edition of the bank quiz, which was rolled out in 2020, was attempted more than 440,000 times.

b) Improved Anti-Scam Protections for E-Commerce Transactions

24. E-commerce scams continue to be one of the top scam types in Singapore. To secure e-commerce marketplaces from scams, the Inter-Ministry Committee on Scams (IMCS) launched the following two initiatives in May 2022:

i. E-commerce Marketplace Transaction Safety Ratings ("TSR"). The TSR informs consumers on the transaction safety of major e-commerce

² Figures updated as of 31 July 2022.

marketplaces, based on the range of anti-scam measures they have in place. Under the TSR Report, these marketplaces have been assigned an overall safety rating, which indicates the extent to which they have implemented anti-scam measures that ensure (a) user authenticity, (b) transaction safety, (c) availability of loss remediation channels for consumers, as well as (d) the effectiveness of their anti-scam measures. E-commerce marketplaces with all the critical anti-scam measures in place will be awarded the full four-ticks. We have also included marketplace-specific advisories to reflect the safety features that are deployed by the individual e-commerce marketplaces. The TSR can be found at the following link: "https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings" and will be reviewed annually. (See Annex C for the findings of the latest TSR.)

ii. For the inaugural TSR, the e-commerce marketplaces have been rated as follows:

Rating	E-Commerce Marketplace			
~ ~ ~ ~	Amazon, Lazada, Qoo10			
\checkmark \checkmark \checkmark	Shopee			
v v	Carousell			
¥	Facebook Marketplace			

iii. Revised Technical Reference 76 on Guidelines for Electronic Commerce Transactions ("TR 76"). The national standard for ecommerce transactions, TR 76, has been revised to include additional anti-scam guidelines that e-retailers and e-commerce marketplaces can put in place to secure e-commerce transactions, and offer better protection for consumers transacting online. These best practices secure different areas of transactions, covering pre- and post-purchase activities, customer support and merchant verification.

25. Members of the public are advised to keep themselves informed of the latest scam variants. They can visit the website <u>www.scamalert.sg</u> to learn about the various scam types and steps they can take to avoid falling prey.

Rise in Outrage of Modesty Cases

26. Outrage of modesty (OM) cases increased to 773 in the first half of 2022, from 739 cases in the same period last year.

27. Of the 773 OM cases in the first half of 2022, 489 cases involved culprits known to the victim, while 284 cases involved culprits unknown to the victim.

28. Although the number of OM cases occurring within the public transport system fell to 80 cases in the first half of 2022, from 87 cases in the same period last year,

OM remains a concern. Most of these cases in the public transport system involved culprits unknown to the victims.

29. The Police continue to work closely with public transport operators and partners, including NCPC, to reach out to commuters to raise awareness, such as through posters on OM, which are prominently displayed on MRT trains. Over the next few months, the Police will launch new public education videos on OM at MRT stations, and continue to 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.

30. Riders on Watch (ROW), a programme that has been subsumed under the Community Watch Scheme (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.

31. Victims of molestation are advised to make a police report as soon as possible as reporting such crimes early is crucial in helping the Police identify and arrest the perpetrators. For example, providing information on the suspect's appearance, attire, height or any other distinctive physical features would be helpful in Police's investigations.

Decrease in Voyeurism Cases

32. Voyeurism cases decreased to 216 in the first half of 2022, from 236 cases in the same period last year. This could be partly due to public education efforts on increasing crime awareness.

33. Although voyeurism cases registered a decline, voyeurism cases by unknown culprits saw a slight increase of 5 cases in the first half of 2022, from 138 cases in the same period last year. Locations which are prone to voyeurism cases committed by unknown culprits were:

- a) on the public transport system, where 34 cases were reported in the first half of 2022, as compared to 41 cases in the same period last year;
- b) in residential premises, where 28 cases were reported in the first half of 2022, as compared to 21 cases in the same period last year; and
- c) in shopping complexes, where 26 cases were reported in the first half of 2022, as compared to 21 cases in the same period last year.

34. Members of the public are reminded to stay vigilant against voyeurism by being aware of their surroundings, and advised to make a police report as soon as possible if they are a victim or have witnessed the crime being committed. Reporting such crimes early is crucial in helping the Police identify and arrest the perpetrators.

Cyber Extortion Cases Remain a Concern

35. The number of cyber extortion cases increased to 203 in the first half of 2022, from 138 cases in the same period in 2021. 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 more than \$754,000. Instagram was observed to be the most common platform by which victims were first approached by the culprit, followed by Facebook and Tinder.

36. The Police have been working with NCPC to reach out to members of the public, to alert them to the threat of cyber extortion and educate them on crime prevention measures. The Police will be rolling out targeted advertising on online platforms to raise awareness of cyber extortion and emphasise public vigilance. The Police are also working with the grassroots community to better educate members of the public about this crime and the preventive measures to adopt.

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

37. 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.

38. Family members and friends can play a part too. They can prevent those around them from falling victim to crime, by being aware of the crime situation. Members of the public should stay vigilant and report any crime-related information to the Police.

PUBLIC AFFAIRS DEPARTMENT SINGAPORE POLICE FORCE 29 AUGUST 2022 @ 4PM

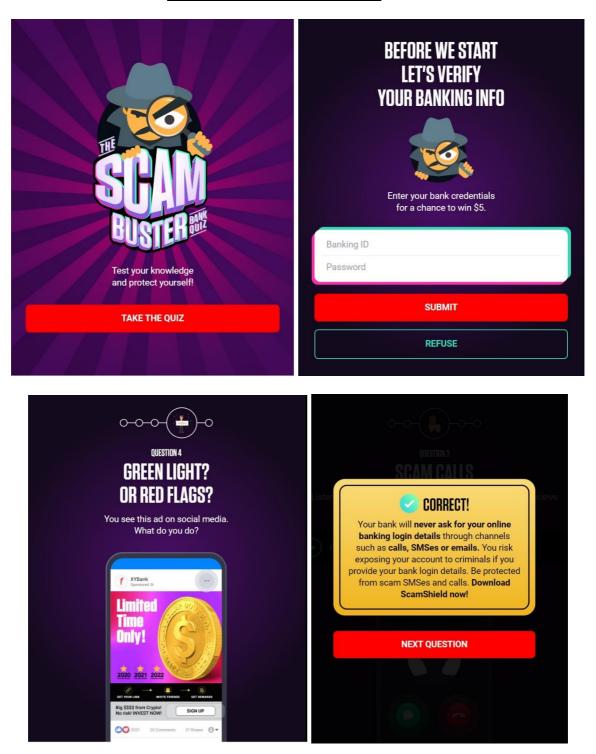
Top 10 scam types in Singapore (Based on number of reported cases)

	Cases Reported			Total Amount Cheated (at least)			Largest Sum
Types of Scams	Jan - Jun 2022	Jan - Jun 2021	Jul - Dec 2021	Jan - Jun 2022	Jan - Jun 2021	Jul - Dec 2021	Cheated in a Single Case in First Half of 2022
Job scams	3,573	481	4,069	\$58.5M	\$6.6M	\$84.3M	\$2.4M
Phishing scams	2,301	1,102	3,921	\$7.8M	\$6.7M	\$28.0M	\$400K
E-commerce scams	2,267	1,057	1,672	\$8.3M	\$2.4M	\$3.4M	\$1.0M
Investment scams	1,683	1,021	1,446	\$108.8 M	\$70.8M	\$119.4M	\$12.0M
Social media impersonation scams	971	961	653	\$2.0M	\$2.9M	\$2.6M	\$243K
Fake friend call scams	717	34	652	\$3.3M	\$99K	\$4.4M	\$124K
Loan scams	571	1,037	1,236	\$4.1M	\$9.6M	\$8.6M	\$160K
Internet love scams	477	546	548	\$20.7M	\$24.9M	\$21.7M	\$1.7M
Credit-for-sex scams	313	329	299	\$950K	\$672K	\$646K	\$55K
Fake gambling platforms scams	308	229	446	\$13.1M	\$17.5M	\$21.5M	\$1.3M
Top 10 scams	13,181	6,797	14,942	\$227.8 M	\$142.5 M	\$295.0M	-

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

Annex B

The Scam Buster Bank Quiz





Annex C

E-commerce Marketplace Transaction Safety Ratings (TSR)

1. The TSR informs consumers on the transaction safety of different e-commerce marketplaces, based on the range of anti-scam measures they have in place. It covers major e-commerce marketplaces that facilitate online transactions from multiple sellers to multiple buyers, with a significant local reach or a significant number of e-commerce scams reported. The TSR microsite can be found at the following link: https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings.

2. The TSR comprises an overall rating and general consumer advisory that will be refreshed annually, as well as marketplace-specific consumer advisories that will be updated every six months.

a. <u>Overall rating</u>. E-commerce marketplaces will be assigned an overall rating, which indicates the extent to which they have implemented anti-scam measures that ensure (a) user authenticity, (b) transaction safety and (c) availability of loss remediation channels for consumers, as well as (d) the effectiveness of their anti-scam measures. E-commerce marketplaces with all the critical anti-scam measures in place will be awarded the full four-ticks. For the inaugural TSR, the e-commerce marketplaces have been rated as follows:

Rating	E-Commerce Marketplace		
~ ~ ~ ~	Amazon, Lazada, Qoo10		
\checkmark \checkmark \checkmark	Shopee		
~ ~	Carousell		
~	Facebook Marketplace		

- b. **Consumer advisory**. General advisories on how consumers may protect themselves when transacting online, as well as the features which keep e-commerce transactions safe, will be published on the TSR microsite.
- c. <u>Marketplace-specific advisories</u>. These advisories will be tailored to reflect the safety features that are deployed by individual e-commerce marketplaces.