feedzai

The State of Scams in Singapore – 2023

GASA
Global Anti-Scam Alliance

Singaporeans Struggle with $2.51 Billion Scam Losses in 12 Months

In the vibrant city-state of Singapore, a dynamic blend of tradition and innovation, a new digital challenge unfolds against the backdrop of dazzling skyscrapers and lush greenery. The 2023 State of Scams in Singapore report, a collaborative effort between the Global Anti-Scam Alliance & Feedzai, not only presents the statistical landscape but also resonates with the resilience of the Singaporean spirit.

Engaging with the experiences of 500 Singaporeans, the study paints a detailed picture. The majority of participants, skewed toward men in the 25-34 age group with a University Degree, form the backbone of the surveyed population.

Singaporeans exude confidence in their ability to identify scams, with a striking 68% feeling (very) confident. Conversely, only 8% admit to not feeling confident at all. However, these self-assured citizens face a stark reality, as 68% encounter scams monthly, and 19% experience scam attempts every few months. A concerning 59% witnessed an increase in scams over the last year, with only 14% reporting a decrease.

Scams permeate everyday life through various channels, with phone calls (71%) and text messages (66%) leading the pack. Instant messaging apps (54%), emails (41%), and social media posts (34%) also serve as common conduits. WhatsApp (55%) and Facebook (37%) emerge as scammers' preferred platforms, followed closely by Gmail (29%), Telegram (29%), and Instagram (19%).

Identity theft is the most common scam in Singapore, impacting 25% of participants. Investment scams (15%) and shopping scams (13%) trail behind. The human toll of scams is palpable, with victims recounting tales of financial loss and emotional distress.

A staggering 48% of victims choose not to report scams, citing reasons ranging from familial disclosure to doubts about the efficacy of reporting. Only half of the victims report the scam to law enforcement or government authorities. The government's actions, perceived as (very) bad by 11%, have garnered mixed reactions, with 59% expressing satisfaction.

Survey statistics reveal a financial impact, with 13% of those approached reporting monetary losses, averaging $4,031. Extrapolating to the larger population, approximately 621,872 Singaporeans over 18 have fallen victim to scams, resulting in a total loss of $2.5 billion, equivalent to 0.5% of the nation's GDP.

Despite the prevalence of scams, recovery efforts still need to be completed, with only 9% successfully reclaiming lost funds. An emotional toll looms large, as 54% of victims report a (very) strong emotional impact, while 9% remain relatively unaffected.

The complexity of scams often leaves victims grappling with the aftermath, as many struggle to identify deceit and lack the knowledge to spot fraudulent activities. Common scam checks include the adage "if it's too good to be true, it probably is," alongside visits to anti-scam organization websites.

Reporting mechanisms vary, with victims turning to local police departments, banks, and dedicated platforms like ScamShield. However, complex reporting processes deter some, with 11% expressing dissatisfaction with the authorities' ability to apprehend scammers.

In conclusion, the 2023 State of Scams in Singapore report not only unveils the prevalence and impact of scams but also serves as a rallying call. Singaporeans, known for their tenacity, are urged to enhance public awareness, bolster digital literacy, and simplify reporting mechanisms to navigate the evolving digital landscape successfully. The establishment of the Anti-Scam Command represents a leap forward in uniting law enforcement and financial institutions, thus streamlining anti-scam efforts. Furthermore, the national "I can ACT Against Scams" campaign has been instrumental in equipping individuals with the knowledge and tools to proactively defend themselves against scams.

Looking forward, Singapore aims to elevate its defense against scams through enhanced international cooperation, particularly in the realm of cross-border enforcement and asset recovery. This global partnership aims to expedite the identification, tracking, and freezing of scam-related assets. Moreover, there is a concerted effort to establish international standards for preventative measures, advocating for stringent identity verification protocols on online platforms to deter the proliferation of fraudulent accounts. The recalibration of security measures will prioritize pre-emptive actions over reactive solutions, seeking a harmonious balance between user experience and robust security. These planned initiatives not only underscore Singapore’s commitment to safeguarding its citizens but also reflect a proactive stance in the global fight against scams.

Jorij Abraham

Jorij Abraham
Managing Director
Global Anti-Scam Alliance & ScamAdviser.com

Singaporeans Struggle with $2.51 Billion Scam Losses in 12 Months

Every year, GASA gathers rich, country-specific insights to inform diverse organizations about top scam trends. Feedzai is incredibly proud to be a part of this year's report and play a role in informing fraud strategies to enhance the global fight against scams.

In this year's report, we see that 68% of Singaporeans experience a scam on a monthly basis. Unfortunately, 48% of Singaporeans don't report scams to law enforcement because 1) they think the process is too complicated, or 2) they weren't sure it was truly a scam. A little over 50% of Singaporeans turn to their local police department when they fall victim to scams, while 33% report it to their bank. This means that financial institutions have a unique opportunity to build and sustain trust among their customer base. The way financial institutions handle these delicate situations would either make or break the customer relationship, as 77% of people would leave their bank if they were not refunded for a scam loss. Financial institutions play a pivotal role in not only helping consumers through the remediation or reimbursement process, but also protecting them from future scams. Governing authorities believe in this sentiment as well.

In example, the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) proposed a Shared Responsibility Framework. This framework includes financial institutions and telcos – both play critical roles facilitating the money from scams and providing the infrastructure for SMS, which is often used by scammers.

We need a collaborative approach to stand a chance in the fight against scams. This means banks, big tech companies, telcos, regulators, and consumers must work together to end the scams contagion. During GASA's most recent in-person conference in Lisbon, they brought together scam-fighting leaders across major companies, like Amazon, Meta, and more, to discuss the future of scam prevention.

In the meantime, what fraud prevention methods can financial institutions utilize to protect customers?

1. **Continuous, customer-centric risk scoring:** Each consumer has their own unique banking behavior. Learn and analyze what their baseline behavior looks like to effectively identify suspicious anomalies. Machine learning technology relieves banks of the heavy lifting by spotting patterns in large volumes of data.

2. **Behavioral biometrics and transactional patterns:** Analyze how the consumer digitally interacts with your banking mobile app or website – time of logins, keystrokes, typing patterns, velocity of payments, addition of new beneficiaries, and more. This contextual information on both the banking session and payment allows financial institutions to detect scams further upstream.

3. **Consumer education:** Financial institutions can deploy a variety of scam education tactics. At minimum, banks can display warning messages before the consumer can complete the transaction. But other banks have email campaigns to inform consumers about the latest scam trends, its scale, and how they can stay vigilant.

Scammers are relentlessly targeting consumers; do not let your guard down. There are numerous types of scams that financial institutions should be vigilant against. Learn about the different types of scams and how to combat them here.

Feedzai is a proud partner of GASA and aims to equip financial institutions with the tools they need to prevent scams and protect consumers. Learn more about Feedzai here.

David Haynes
Vice President and General Manager of Asia Pacific
Feedzai

Singapore's Ministry of Home Affairs Spearheads Bold Initiatives Against Rising Scams

Singapore, known as a haven of safety and security, hasn't been immune to the challenges of the digital era. Despite being recognized as the safest country globally in 2022, Singapore has witnessed a surge in online scams, which have become a principal factor driving the national crime rate. Director of Policy Development & Security at the Ministry of Home Affairs Dr Ng sheds light on this issue and the measures being taken to counteract it.

Singapore was named the safest country globally in 2022 by the Gallup Global Law and Order Report. However, the surge in scams challenges this status. How rampant have scams become in Singapore recently? Scams have grown at an alarming rate in Singapore. In contrast to our stable physical crime rates, scams have escalated over the past five years, with reported cases rising fivefold and losses quadrupling. In 2022 alone, there were 31,728 reported cases , a 32.6% rise as compared to 2021. Notably, platforms like WhatsApp, Telegram, and Facebook became hotspots for scammers to perpetuate their scams.

What were the major scams in Singapore in 2022 and their impact? In 2022, Singapore saw a surge in phishing scams with 7,097 cases resulting in SGD 16.5 million in losses, closely followed by job scams with 6,492 cases and SGD 117.4 million lost. E-commerce scams persisted with 4,762 cases, accumulating SGD 21.3 million in losses, while investment scams led to SGD 198.3 million in losses from 3,108 cases. Fake friend call scams had 2,106 cases, causing SGD 8.8 million in losses.

Could you share some of the steps Singapore has initiated to protect consumers from scams? To combat this menace, the Inter-Ministry Committee on Scams (IMCS) has spearheaded various strategies encompassing prevention, detection, enforcement, and education. The IMCS has initiated collaborative efforts with telecom companies and banks to secure communication infrastructure & banking channels, with measures like blocking spoofed numbers and requiring organisations to register their Sender IDs with the SMS Sender ID Registry (SSIR), to warn consumers about potential scam messages. The launch of the ScamShield mobile application facilitates easy reporting of scam calls & messages. A notable venture was the establishment of the Anti-Scam Command, co-locating police and banks to enhance coordination of anti-scam enforcement & investigations. On the education front, the national "I can ACT Against Scams" campaign launched in January 2023, guides individuals to Add, Check, and Tell - a three-step precautionary process to safeguard against scams.

Such comprehensive measures indeed make a difference. What further actions do you propose to give consumers an upper hand in the fight against scams? Firstly, enhancing our cross-border enforcement capabilities through international collaborations, such as establishing frameworks for swift asset recovery. This will facilitate quicker intervention, tracing the flow of scam proceeds and freezing fraudulent accounts promptly. Secondly, forging global norms for preventative measures against scams, including setting guidelines for online platforms to verify user identities and prevent the creation of inauthentic accounts. A re-calibration of the balance between security and user experience is essential, focusing on preemptive measures instead of post-scam enforcement.

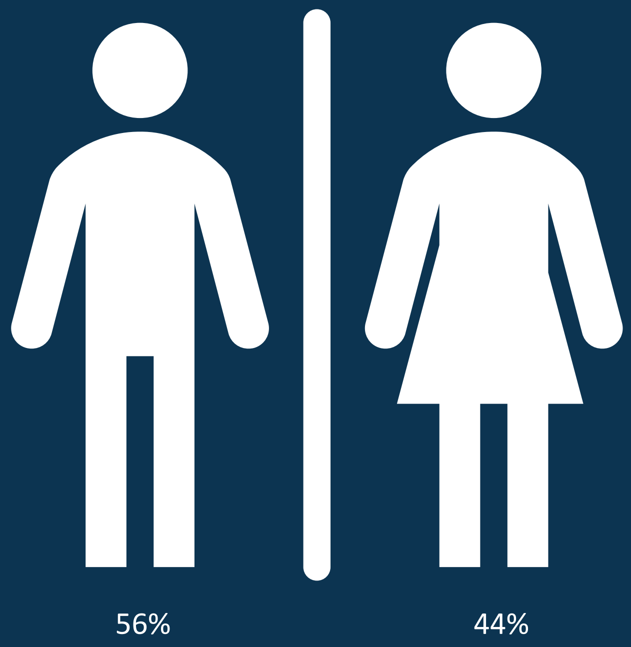
In the face of growing challenges, Singapore, led by vigilant organizations like the Ministry of Home Affairs, continues to innovate and adapt, aiming to maintain its position as a safe and secure nation in the digital era.

Dr. Ng Li Sa
Director of Policy Development & Security, Policy Development Division, Ministry of Home Affairs, Singapore

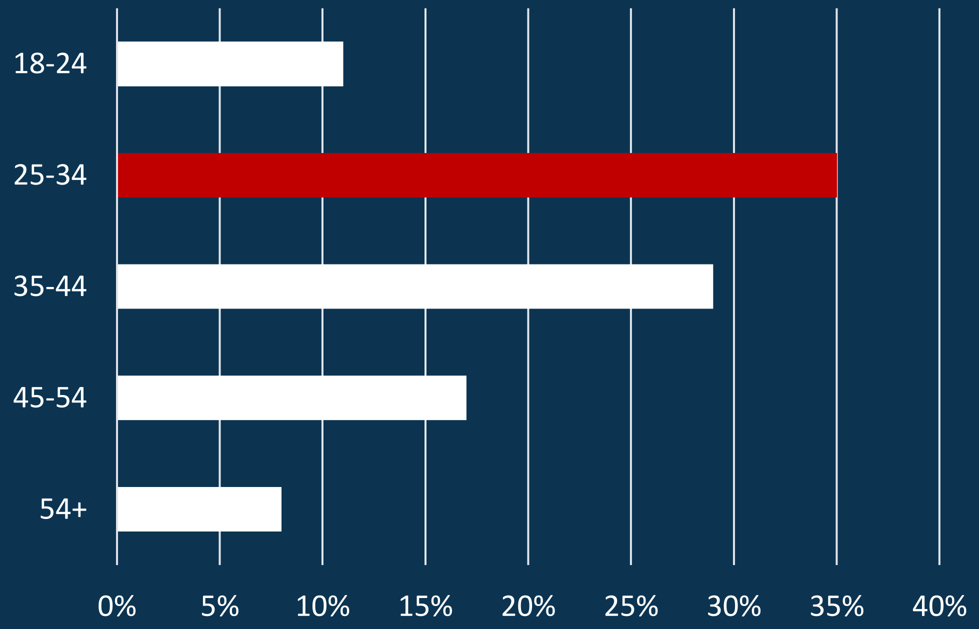
MINISTRY OF HOME AFFAIRS

500 Singaporeans participated in the survey

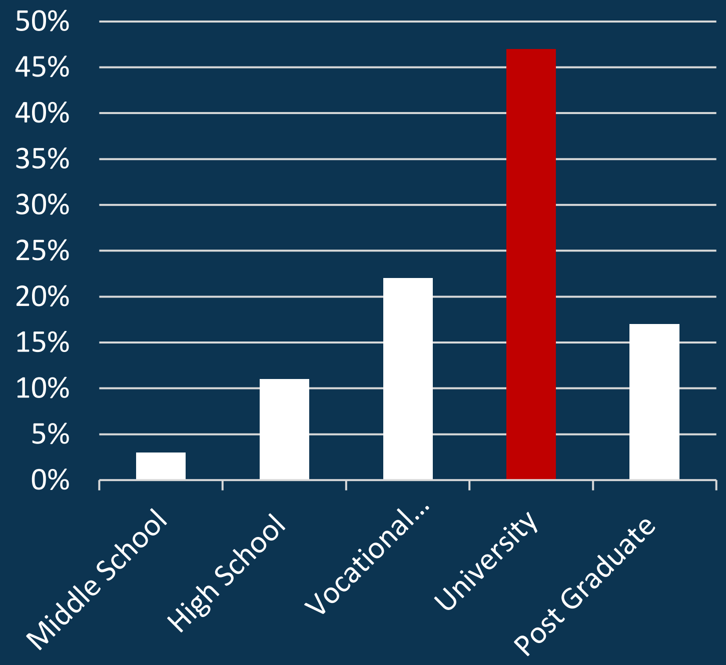
Gender



Age

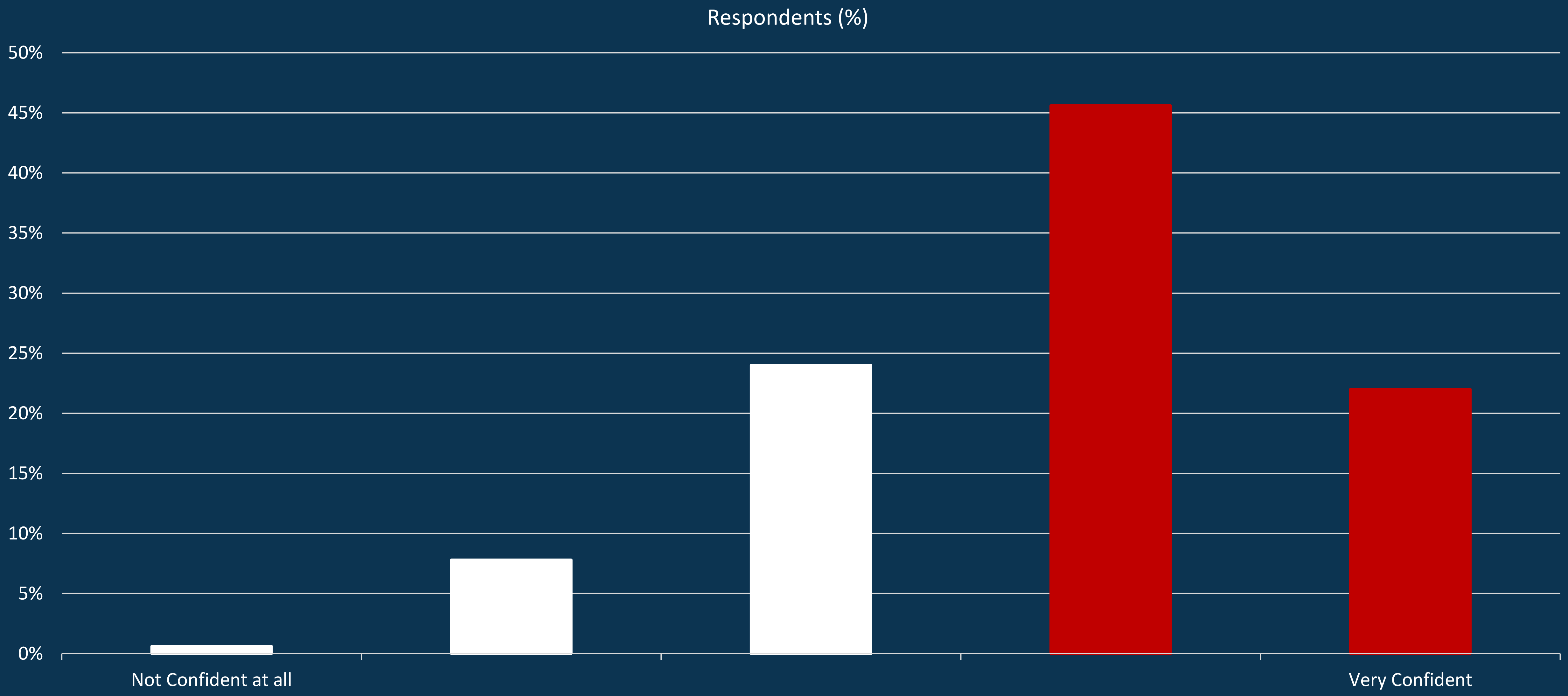


Education



More men than women participated, mainly in the age group 25-34 with a University Degree.

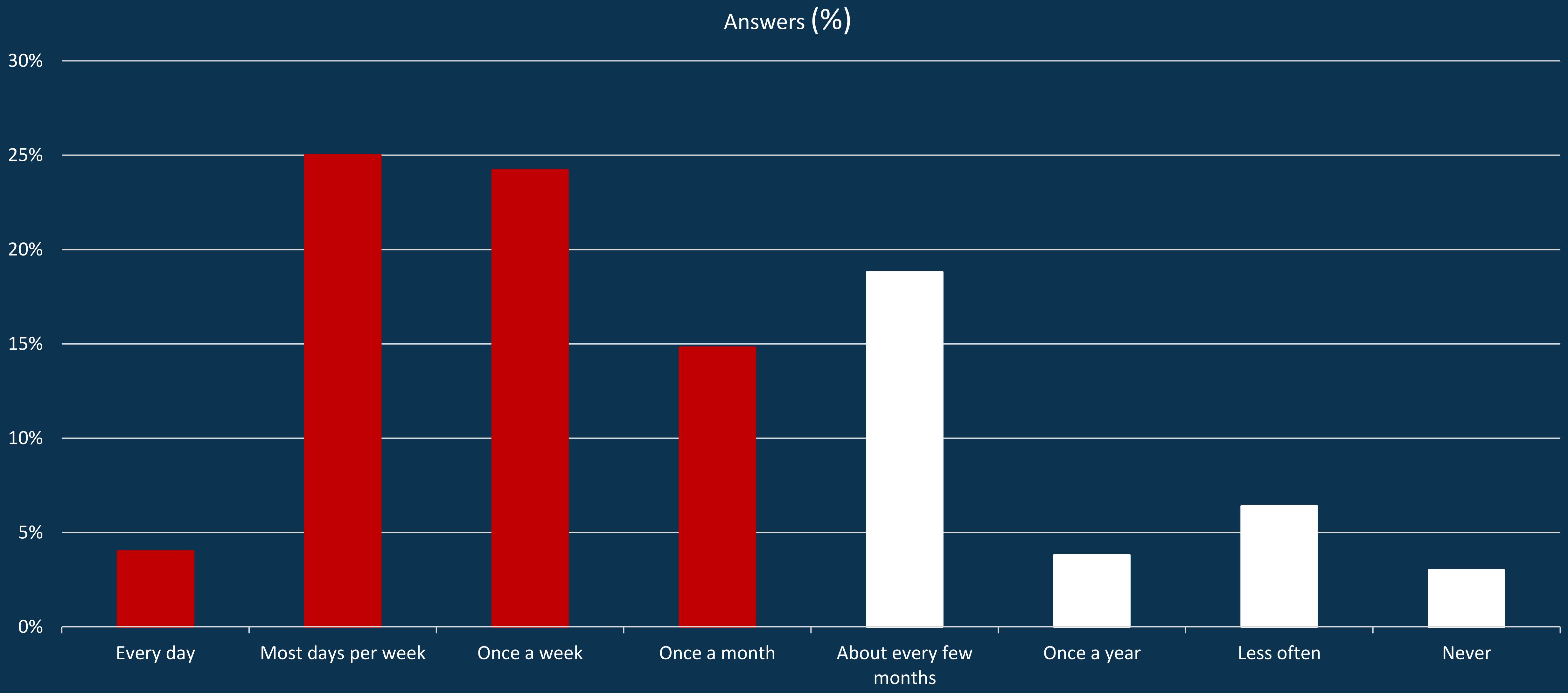
68% of Singaporeans are (very) confident that they can recognize scams



Only 8% are not (very) confident at all.

Q2: How confident are you that you can recognize scams and deceit?

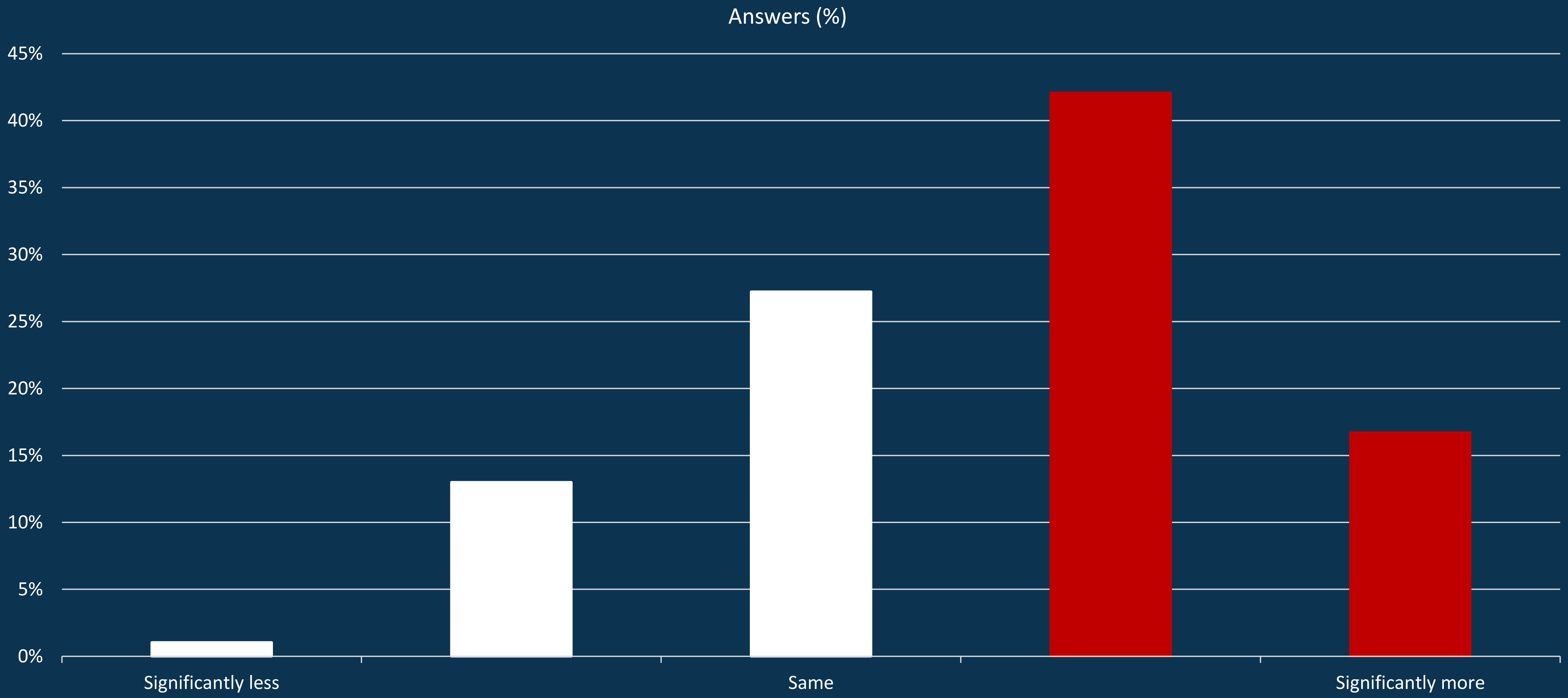
68% of the Singaporeans encounter a scam at least once per month



19% experiences a scam (attempt) at least every few months.

Q3: In the last 12 months, how frequently have you encountered scams including deceptive advertising, phishing/fake emails/texts, phone calls, etcetera)?

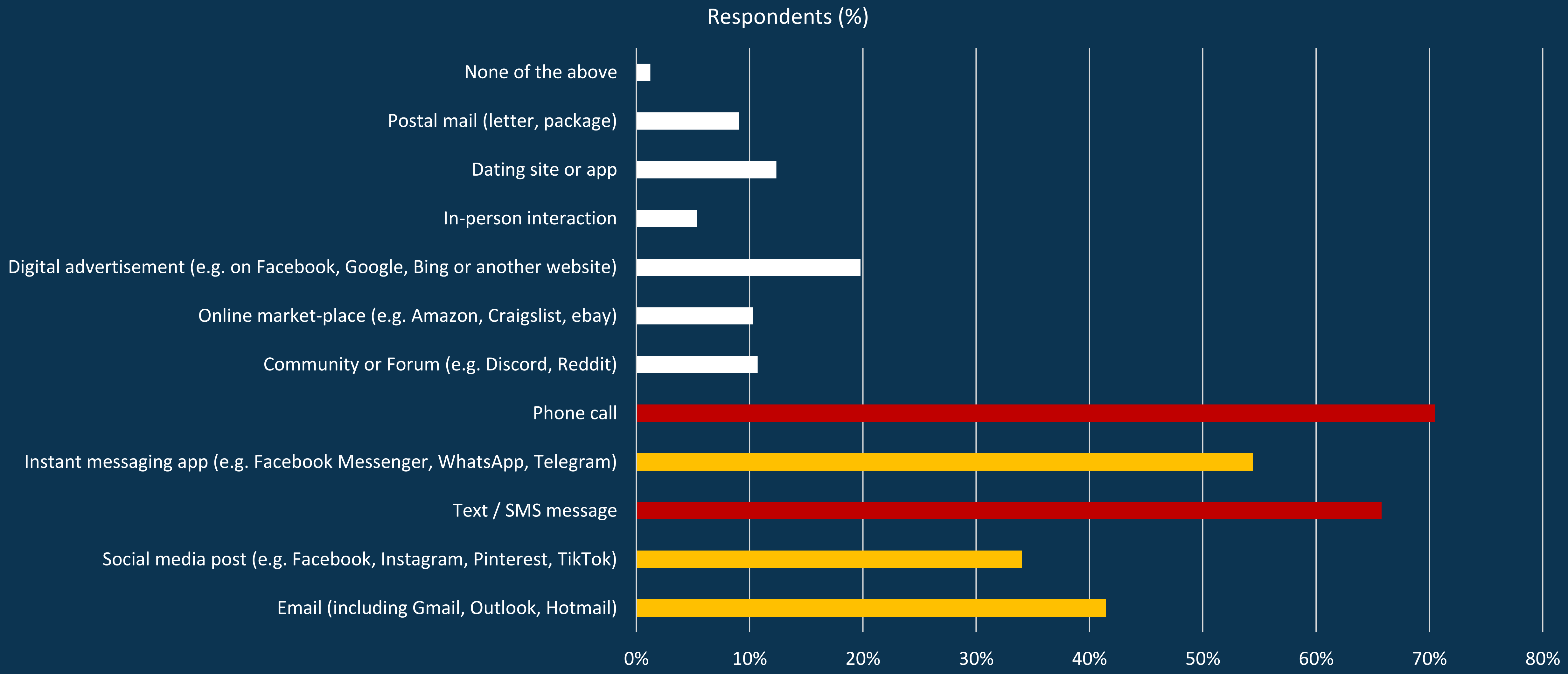
59% of Singaporeans experienced more scams in the last 12 months



Only 14% experienced less scams.

Q4: Compared to the year before, do you feel you have been approached more or less frequently by a individual/company that tried to deceive you in the last 12 months?

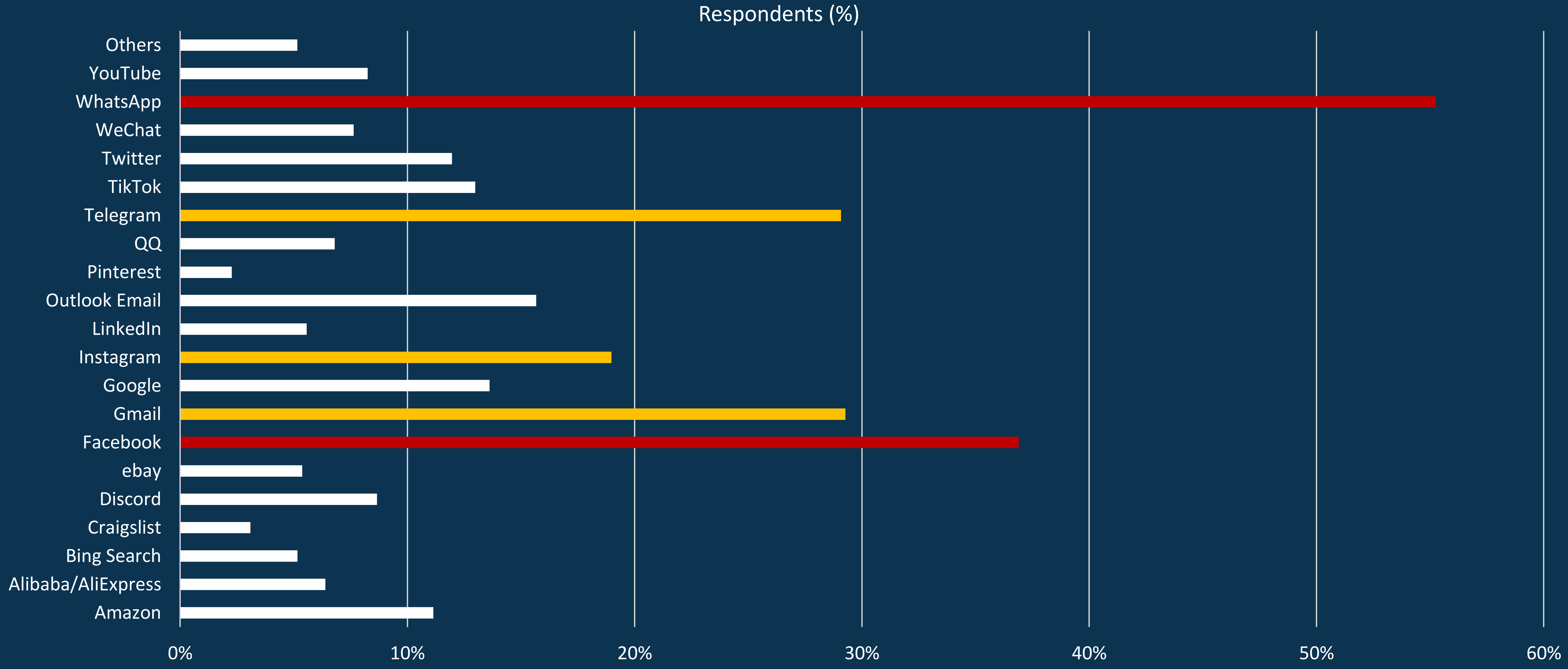
Most Singaporeans receive scams via Phone Calls and Text/SMS Messages



However, Instant Messaging Apps, Emails, and Social Media Posts are also common scam media.

Q5: Through which communication channel(s) did scammers mostly try to approached you in the last 12 months? Choose up to 3.

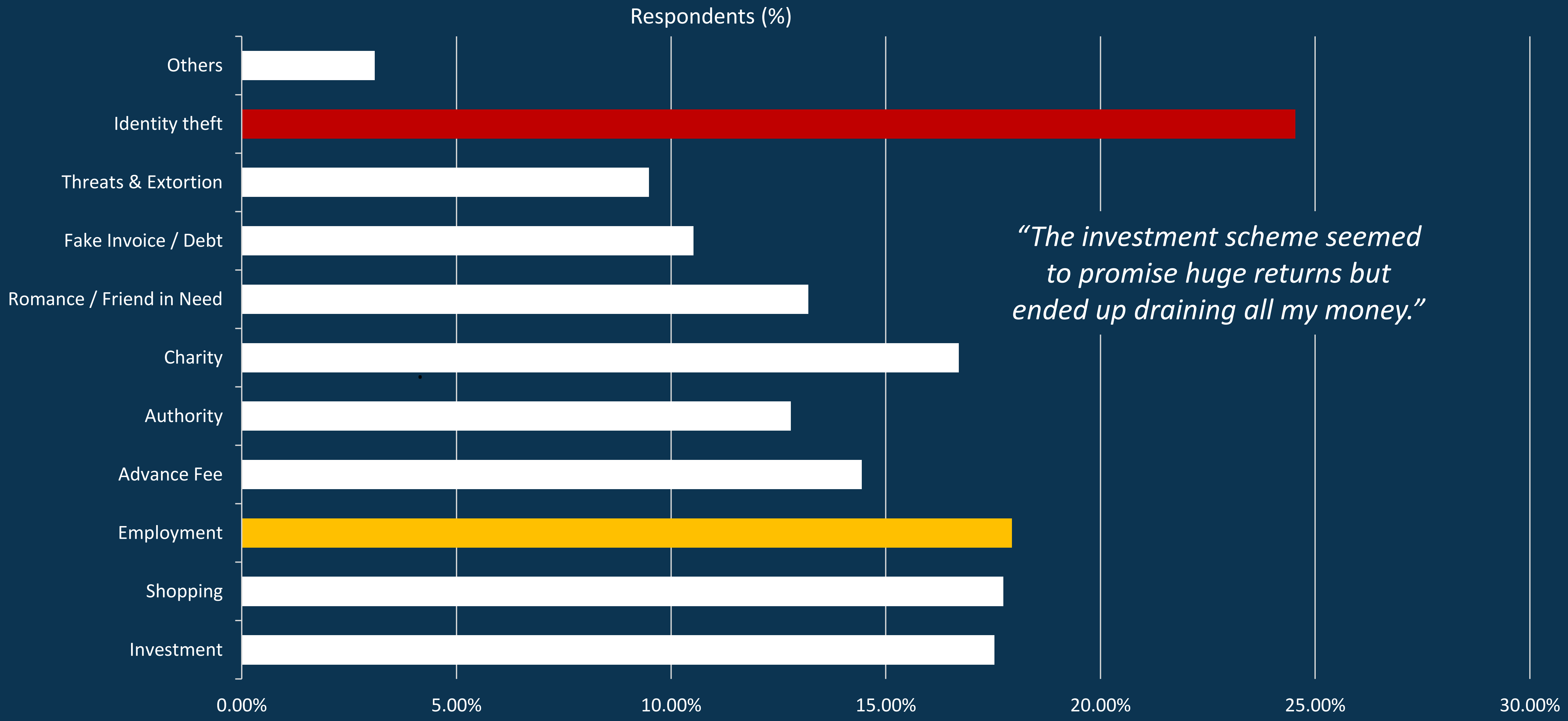
WhatsApp and Facebook are the platforms most exploited by scammers



Gmail, Telegram, and Instagram take 3rd to 5th place.

Q6: Via which platform(s) did scammers mostly try to contact you in the last 12 months? Choose up to 3.

Identity Theft is the most common scams in Singapore

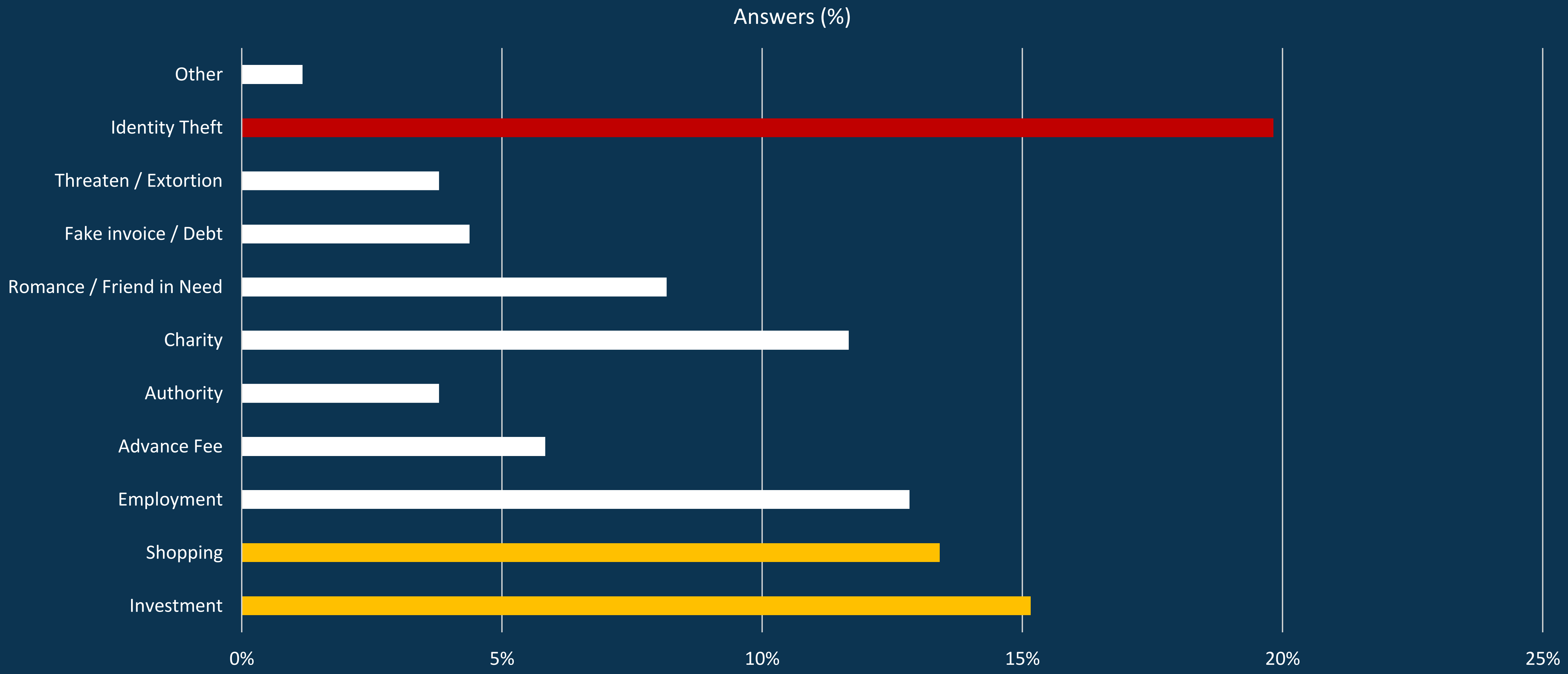


“The investment scheme seemed to promise huge returns but ended up draining all my money.”

29% states none of the scams happened to them in the last 12 months. 1.6 scams were reported per participant.

Q7: Which of the following situations happened to you in the last 12 months? Select all that apply.

Identity Theft has the most impact compared to other scams



Followed by Investment and Shopping Scams.

Q8: Which of the incidents you experienced did have the most impact on you?

Scams are hurting Singaporeans in many ways

"I was approached by a lot of so-called investors or NFTs art curators and they forced me to pay a large sum of money for a process that has (now) been halted.”

“I donated to a charity that turned out to be a fraud."

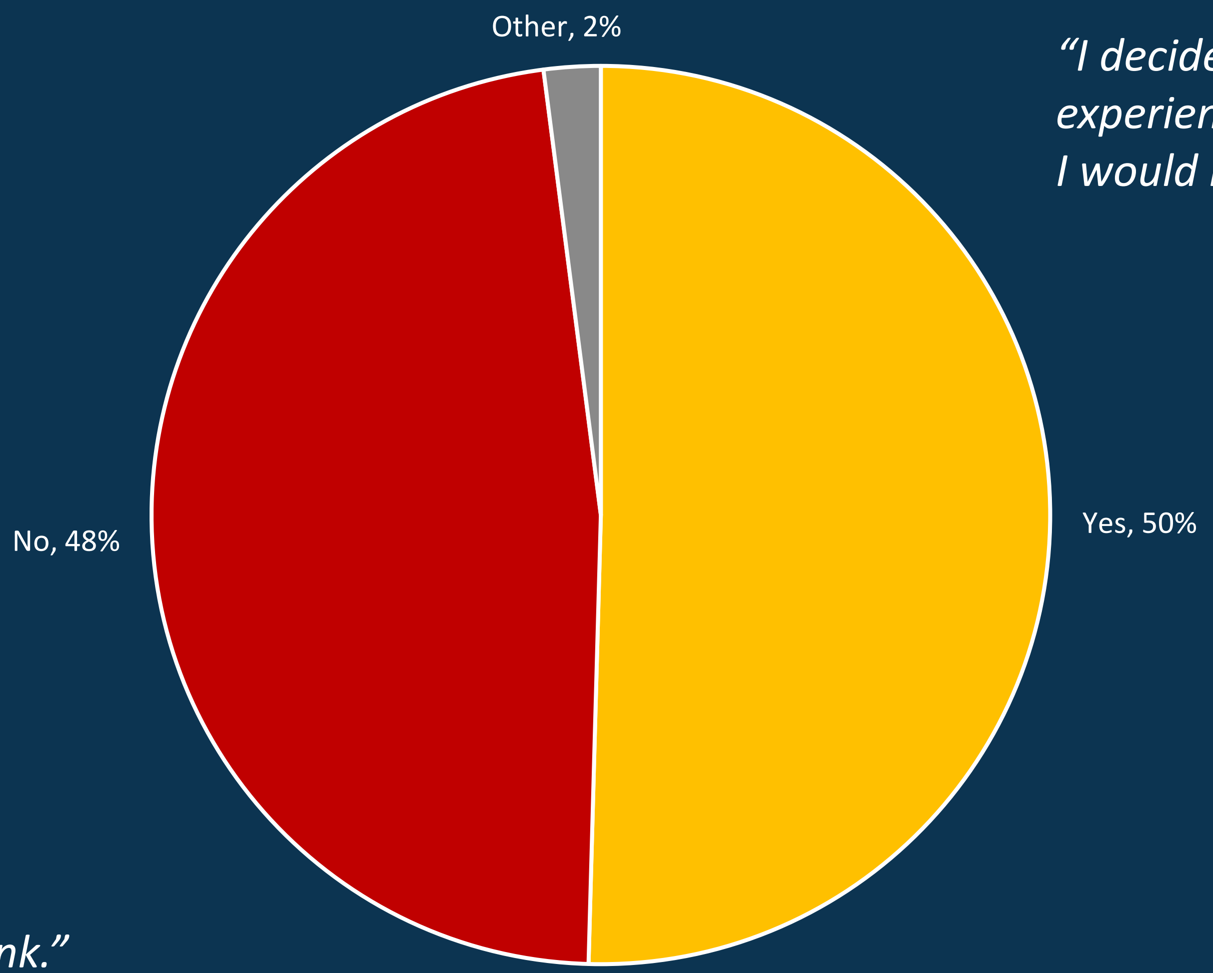
"I was contacted on Twitter by someone I didn't know, claiming I'd won a prize. They directed me to a website to claim it. After I entered my personal information, (They claimed) I needed to pay taxes, After sharing my personal info and paying taxes, they disappeared. Later, I realized it was a scam."

" The goods I ordered turned out to be fake.”

"I invested a sum for a guaranteed return. Initially, I received payments and reinvested them, but in the end, I lost it all.”

Q9: Regarding the negative experience that impacted you the most, describe what happened.

48% did not report the scam to law enforcement



“I decided to tell my family members about the experience, I figured why waste my time when I would most likely not get my money back.”

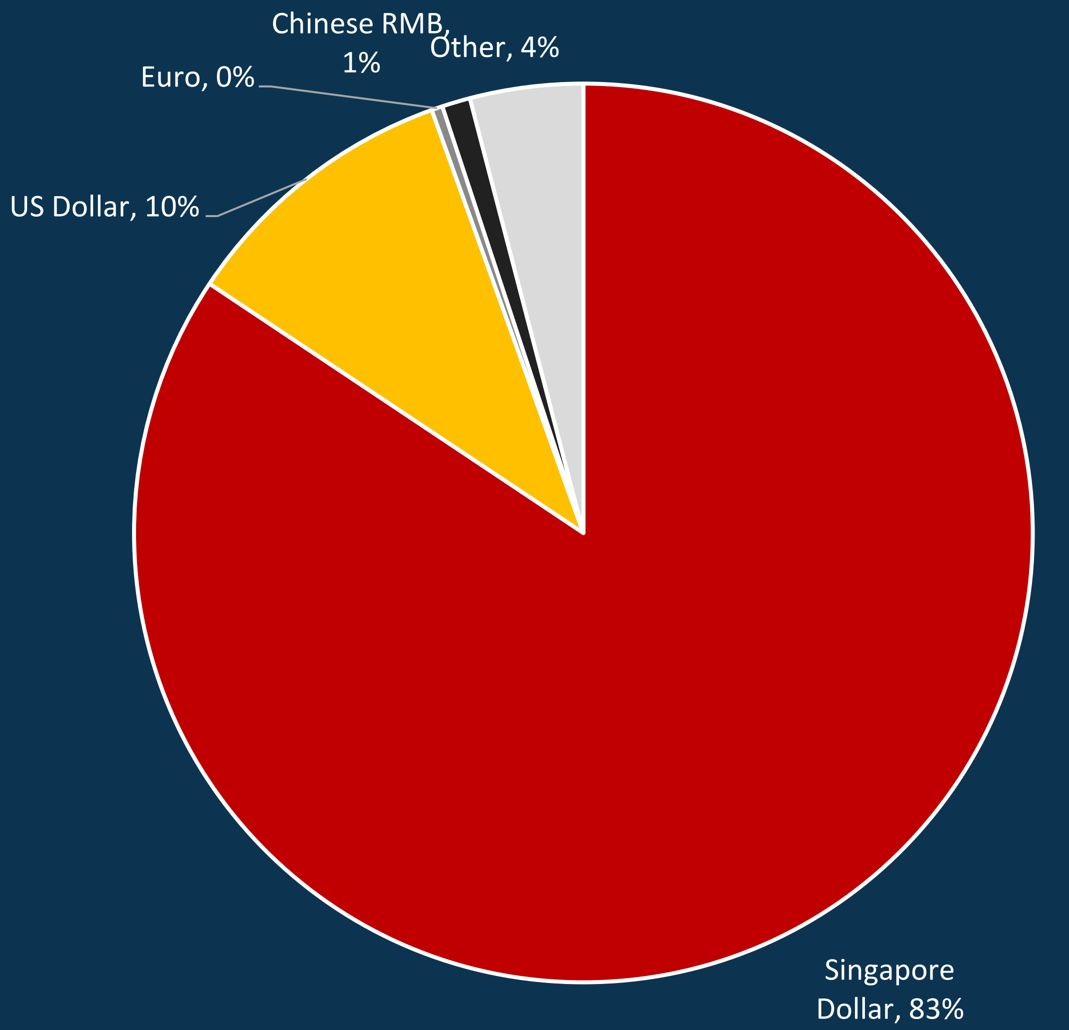
“I filed a report with bank.”

50% stated having reported the scam to law enforcement or another government authority

Q10: Regarding said experience, did you report the incident to law enforcement or another government authority?

In total 13% of the approached persons reported losing money in a scam

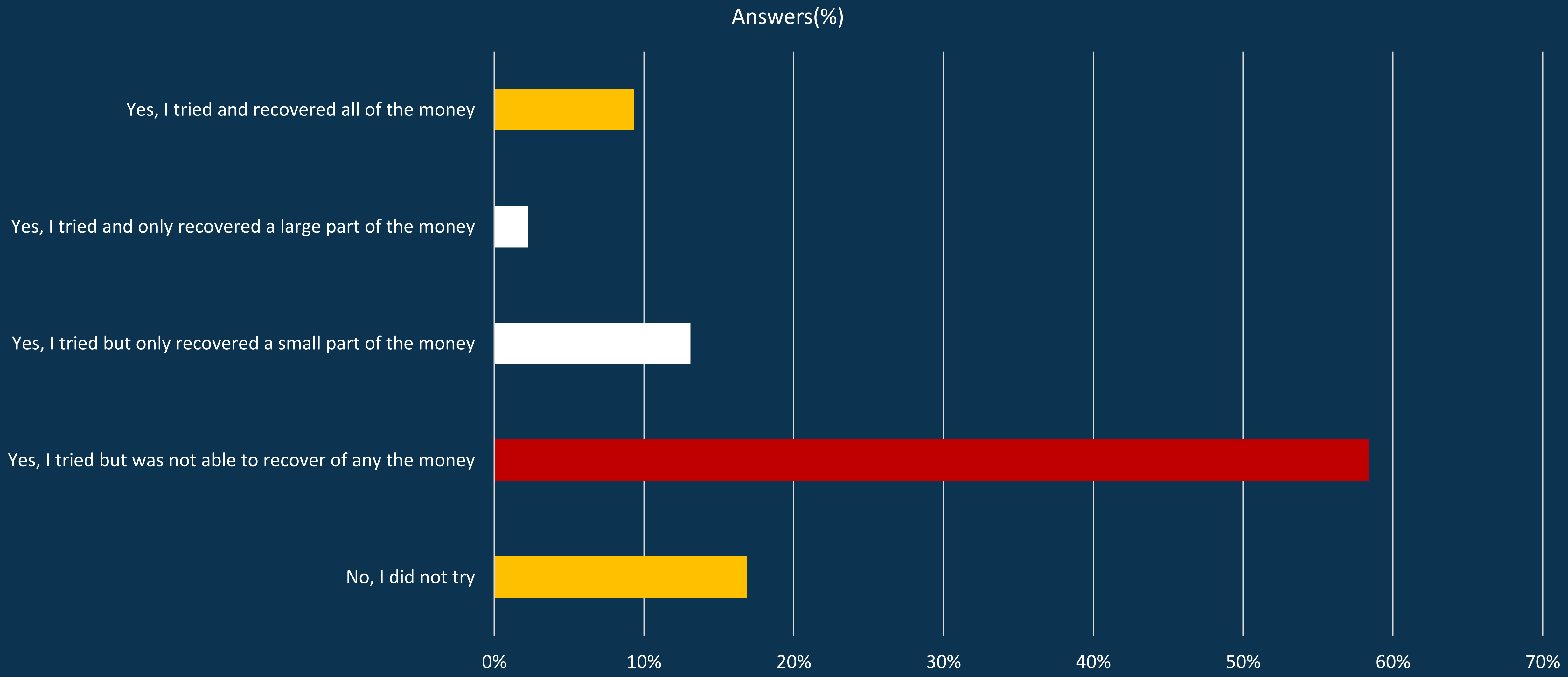
Survey Key Statistics	
Number of persons approached	2,098
Participants completing the survey	34%
Participants losing money	267
% losing money / approached persons	13%
Average amount lost in US Dollars	$ 4,031
Total country population	5,975,383
Population over 18 years	4,886,466
# of people scammed > 18 years	621,872
Total amount lost in scams*	$ 2,506,764,045
Gross Domestic Product ($ millions)	515,548
% of GDP lost in scams	0.5%



Most scams were reported in Singapore Dollars (83%), the remainder is mainly in US Dollars (10%)

Q11 / 12: Think about the incident that has had the most impact. In total, how much money did you lose before trying to recover the funds? Only enter a round number. If no money was lost enter "0".

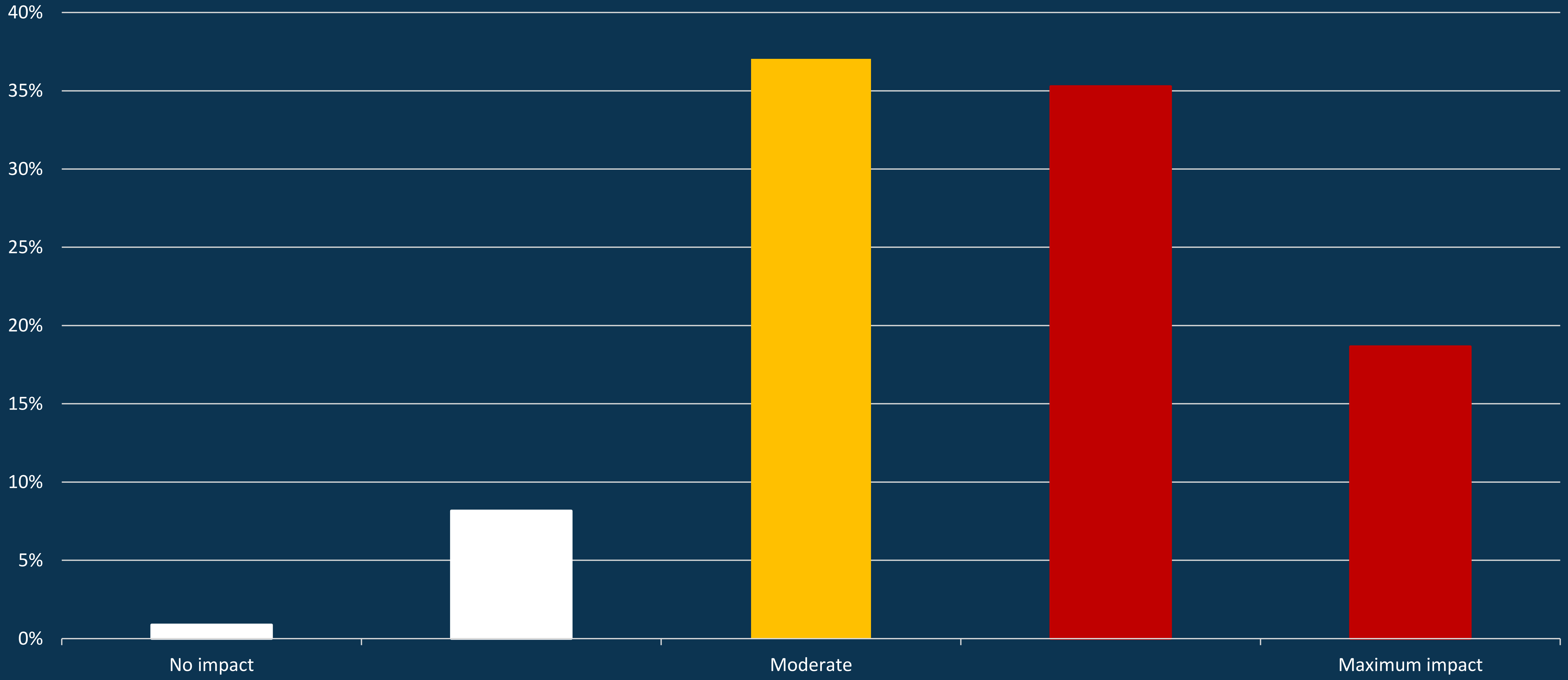
Only 9% of the survey participants were able to completely recoup their losses



17% did not try to recover their funds. 58% tried but was not able to recover any money.

Q13: Did you try to recover the money you lost?

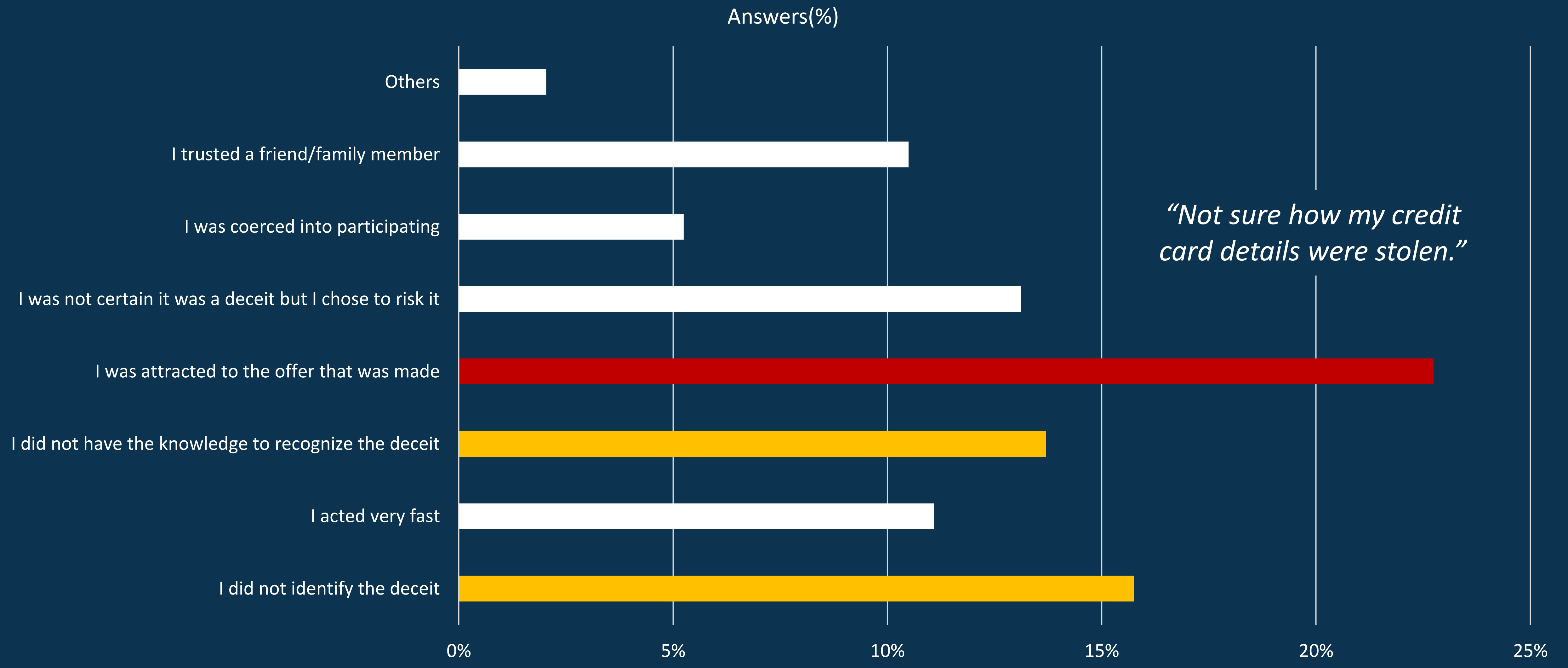
54% of the scam victims perceived a (very) strong emotional impact



9% of the participants reported no or little emotional impact.

Q14: Think about the incident that has had the most impact. To what extent did it affect you emotionally?

The main reason Singaporeans fall for a scam is attraction to the offer

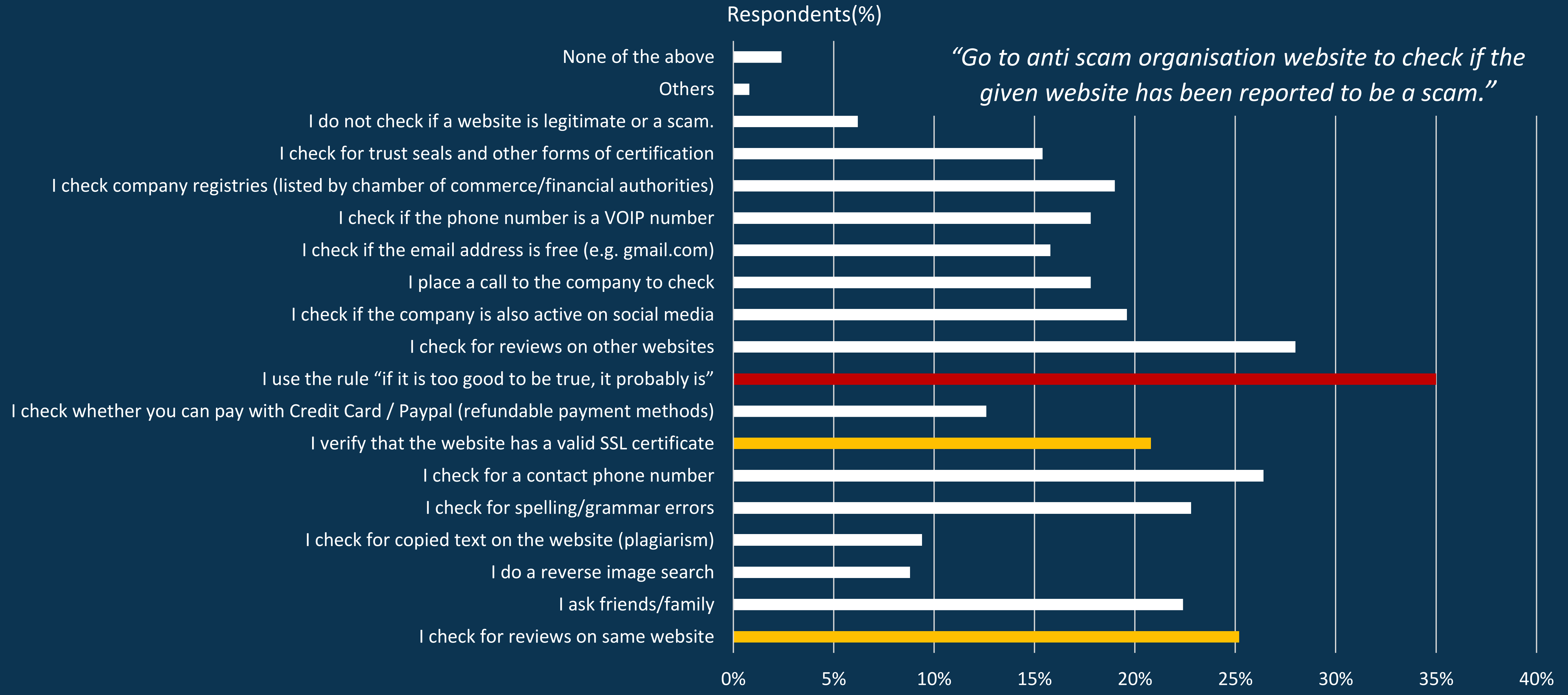


"Not sure how my credit card details were stolen."

Several victims also reported inability to identify deceit and lack of knowledge to identify deceit.

Q15: You stated losing money or personal/financial information in a deceit. What was the main reason this happened?

The most common scam check is ‘if its too good to be true, it probably is’

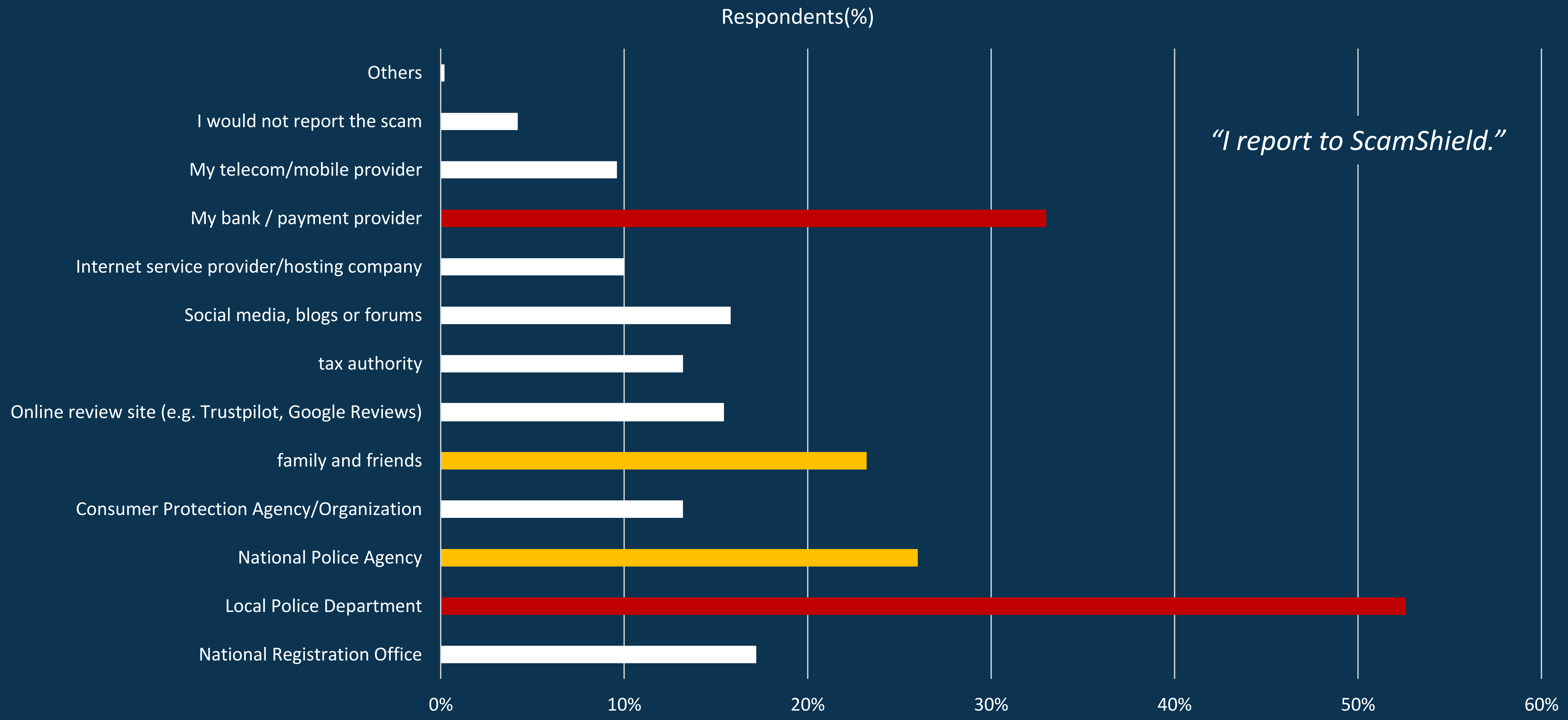


“Go to anti scam organisation website to check if the given website has been reported to be a scam.”

Several “unsafe” methods like checking reviews on the same site and checking the SSL certificate are often used as well.

Q16: Which methods do you usually apply to check if an offer is legitimate or a scam? Select all that apply.

Scams are mostly shared with Local Police Department and Banks

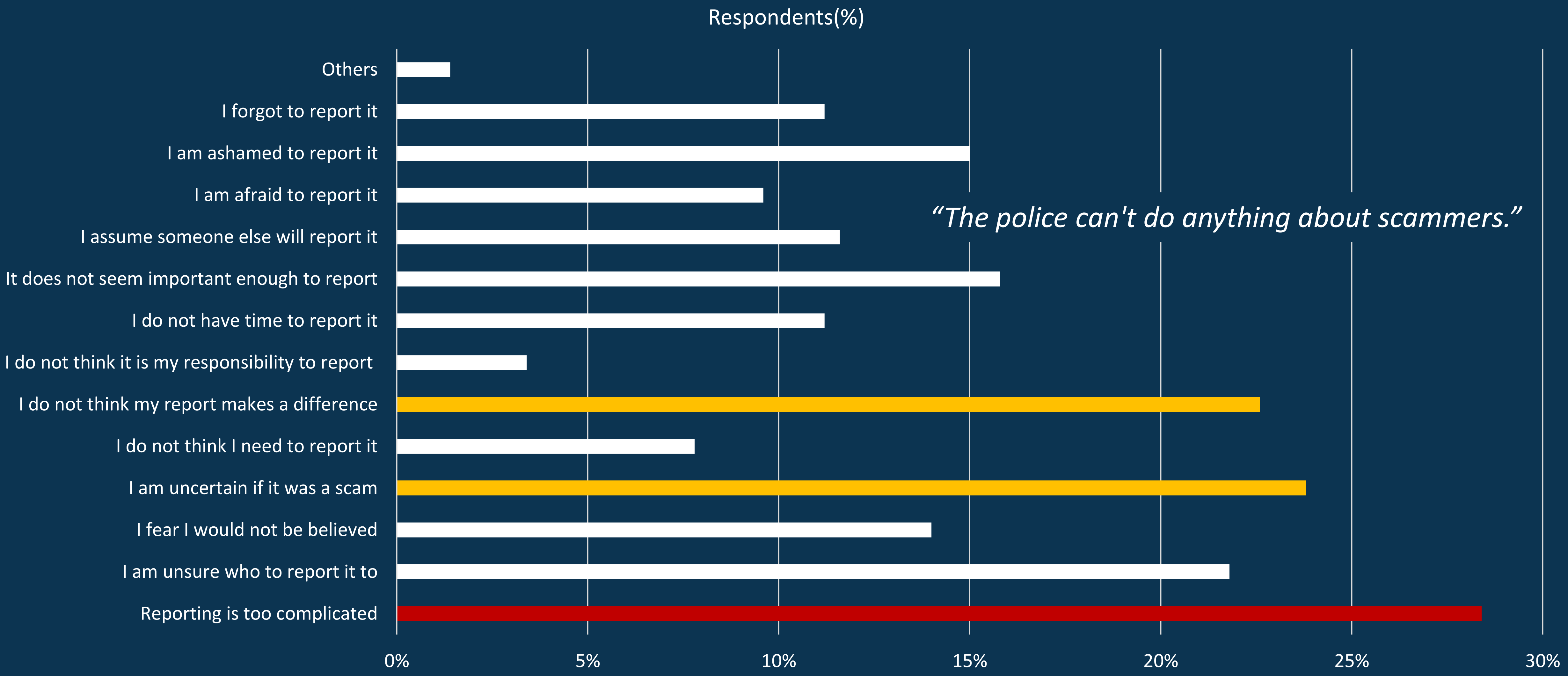


"I report to ScamShield."

Family & Friends and National Police Agency are also popular scam reporting destinations.

Q17: If you were to be deceived, who would you report this to?

The main reason for not reporting scams is complex reporting process

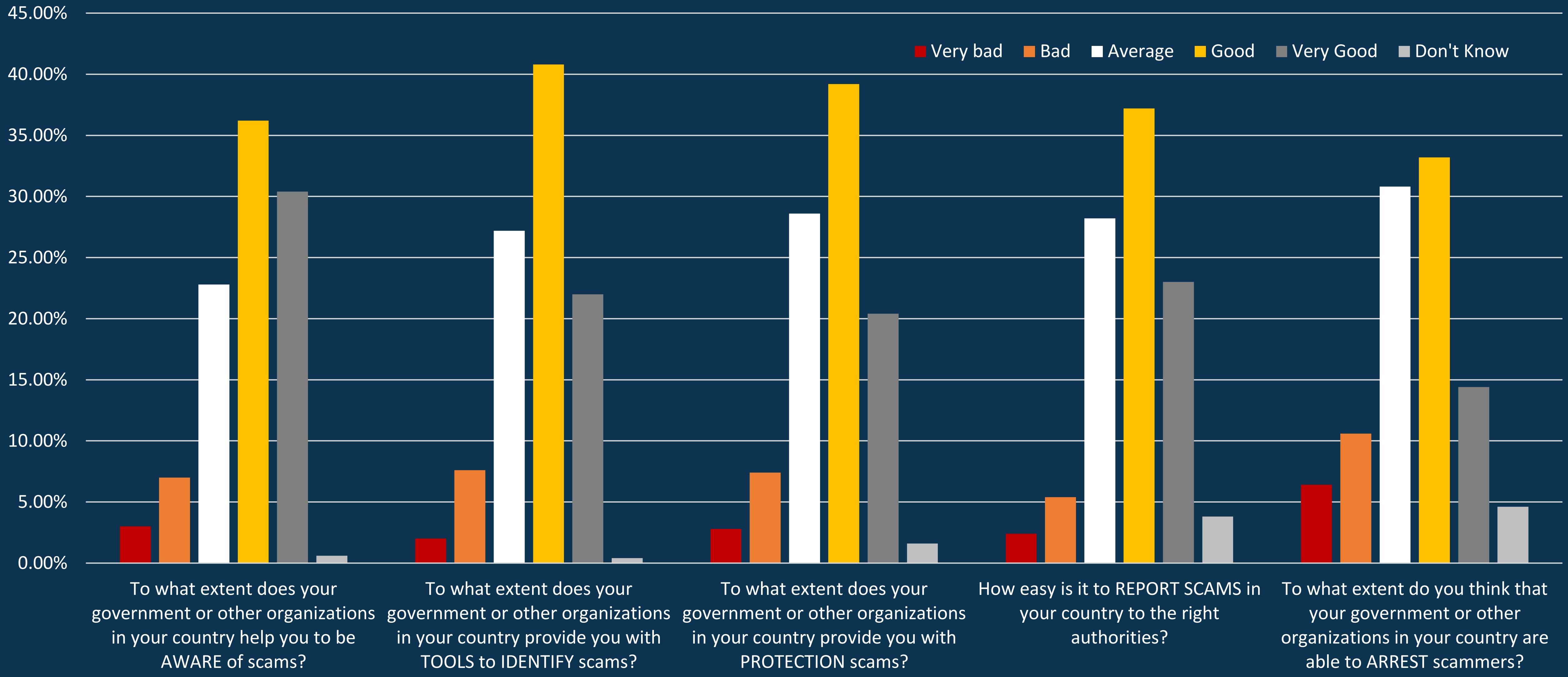


“The police can't do anything about scammers.”

Other key reasons for not reporting are uncertainty if it’s a scam and assuming that reporting won’t make a difference.

Q18: What reasons might you have to not report a scam?

Singaporeans are displeased with their government's efforts to arrest scammers



Overall, 11% of the participants rate the actions of governments as (very) bad, 59% as (very) good

Q19: How would you rate the efforts of your government and other organizations in your country in fighting online scams?

Some remarkable quotes

“Exercise caution and refrain from sharing your identity, contact details, as well as personal and family information with others.”

“When someone asks for money directly, be cautious and don't trust too quickly.”

“I hope the bank can make their app/website more secure. They could add an extra verification question when we log in and use face recognition when we transfer money."

“Reporting is easy, but recovering lost money is challenging.”

“Delete unknown emails immediately, do not enter any data on the Internet, do not pick up unknown phone calls.”

About this Report

Who are we?

GASA
Global Anti-Scam Alliance

The Global Anti Scam Alliance (GASA) is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organizations to share insights and knowledge surrounding scams.

Feedzai is the world’s first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime. Feedzai enables leading financial organizations globally to safeguard trillions of dollars of transactions and manage risk while improving their customers' trust.

feedzai

Special Thanks & Methodology

Special Thanks

We would like to thank Professor Mark Button, Co-Director of Centre for Cybercrime and Economic Crime at the University of Portsmouth, Jack Whittaker, PhD Candidate Criminology at the University of Surrey and Peter Hagenaars of the Dutch Police, for their feedback and support.

Methodology

We used Pollfish.com to set-up the consumer survey and get participants. Pollfish utilizes a survey methodology called Random Device Engagement. RDE is the natural successor to Random Digit Dialing (RDD). Our survey was delivered via Pollfish inside popular mobile apps, RDE utilizes the same neutral environment as RDD, and an audience who are not taking premeditated surveys, by reaching them inside mobile apps they were using anyway.

Pollfish uses non-monetary incentives like an extra life in a game or access to premium content. With additional layers of survey fraud prevention including AI and machine learning, Pollfish removes potentially biased responses, improving data quality even further.

Biases towards a specific age or educational level were statistically corrected based on the general distribution within a country. The estimate how much money was lost remains a difficult question to answer. Depending on the country outliers had to be removed. Also, for bitcoin, it was not possible to report amounts smaller then 1. Hence bitcoin loses were not included in the estimate.

In addition to Pollfish we used the following sources:

- Inhabitants per country: Worldometers.info
- Currency conversion: Xe.com
- The country flag on the cover: wikimedia.org
- Internet penetration: Wikipedia
- GDP Estimate 2023: Wikipedia

The survey itself has been party Inspired by DeLiema, M., Mottola, G. R., & Deevy, M. (2017). Findings from a pilot study to measure financial fraud in the United States. Available at SSRN 2914560.

Feedback is greatly appreciated. You can contact us at partner@gasa.org

About The Authors

Jorij Abraham has been active in the Ecommerce Industry since 1997. From 2013 to 2017 he has been Research Director at Thuiswinkel.org, Ecommerce Europe (the Dutch and European Ecommerce Association) and the Ecommerce Foundation.

Nowadays, he is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.

Marianne Junger is Professor Emeritus of Cyber Security and Business Continuity at the University of Twente. Her research investigates the role of human factors of fraud and of cybercrime, more specifically she investigates victimization, disclosure and privacy issues. The aim of her research is to develop interventions that will help to protect users against social engineering and to increase compliance.

She founded the Crime Science journal together with Pieter Hartel and was an associate-editor for 6 years.

Luka Koning is a Researcher/PhD Candidate at the University of Twente. His research focuses on victimization of fraud and cybercrime, in particular the prevalence, risk factors, impact, and willingness to report. His work includes victim studies and experiments, aimed at how victimization arises and subsequently how it could be prevented.

Clement Njoki is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.

Sam Rogers is Director of Marketing at GASA. Before moving into marketing management, he worked as a copywriter and content manager, specializing in cutting-edge areas of electrical engineering, such as photonics and the industrial applications of electromagnetic radiation. Sam left the world of industry in search of fulfilment and now uses his skills to expose the impact of online scams to a global audience.

Interested in participating in this report next year? Please contact jorij.abraham@gasa.org.

The Global Anti-Scam Alliance is supported by the following organizations

Foundation Partners

amazon

Gogolook

SCAMADVISER

TREND MICRO™

Corporate Partners

AnyDesk

BARCLAYS

BioCatch

cifas
Fighting Economic Crime Together

cira

Crystal

CSC

EBRAND

.eu
Powered by EURid

feedzai

globaleyez | the brand protection experts

GROUP-IB

LexisNexis®
RISK SOLUTIONS

mastercard

REALTIME REGISTER

If you like to become a GASA partner, please contact partner@GASA.org

Disclaimer
This report is a publication by the **Global Anti Scam Alliance** (GASA) supported by **Feedzai**. GASA owns the copyrights for the report. Although the utmost care has been taken in the construction of this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

Global Anti-Scam Alliance (GASA)
Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands
Email: partner@gasa.org
Twitter: @ScamAlliance
Linkedin: linkedin.com/company/global-anti-scam-alliance