The State of Scams in Australia

feedzai

GASA
Global Anti-Scam Alliance

Digital Defenses Needed as Australians Face US$5.58B Scam Losses in 12 Months

In the vast, sun-soaked canvas of the Australian outback, a digital storm is brewing, and it's costing more than just dollars. In the thrilling saga of cyber resilience, the State of Scams in Australia report unfolds, a collaborative masterpiece crafted by the Global Anti-Scam Alliance and Feedzai, enriched with the insights of sharp Aussie minds. Australians, known for their no-nonsense attitude and a fair go ethos, are now facing a US$5.58 billion has been claimed by the relentless wave of scams in the past 12 months.

1,000 Australians took part in the survey. With more women than men, predominantly from the spirited 25-34 age group armed with high school education, they embarked on a journey to unveil the elusive truth behind online deception.

Australians exude a peculiar confidence, a blend of the easy-going Aussie charm and a steely determination. A solid 69% claim they can spot scams from a mile away, but here's the twist — a mere 6% admit they're not confident at all. Amidst this swagger, the harsh reality hits — 75% encounter scams monthly, and 14% face scam attempts every few months. It's like a game of digital cat and mouse, and Aussies are right in the thick of it. A resounding 61% witnessed an increase in scams over the last year, while only 9% reported a decrease.

Text/SMS messages (66%) and phone calls (61%) are the old guns, leading the charge. But, surprise, surprise, emails (61%) and instant messaging apps (23%) aren't far behind. Gmail (43%) and Facebook (35%) are the playgrounds for these digital mischief-makers, with Outlook Email (24%), WhatsApp (19%), and Instagram (12%) playing the sidekicks. Enter the main act: Identity theft, the scourge of consumers in Australia. Picture this — victims not just losing money but grappling with the emotional turmoil of a post-scam world.

Now, let's talk channels. Identity theft stands out as the most common scam in Australia, leaving victims grappling with the aftermath of financial loss and emotional distress. While 45% claim immunity to scams in the last 12 months, the average Aussie victim, though, wears the scars of 1.76 scams.

From a financial perspective, 17% of those approached reported monetary losses, averaging $1,548. Extrapolating to the broader population, approximately 3,601,546 Aussies over 18 have danced with the devil of scams, resulting in a substantial loss of $5.58 billion, equivalent to 0.3% of the nation's GDP.

Recovery remains elusive for many, with only 22% successfully reclaiming lost funds. The emotional toll is pronounced, with 49% of victims reporting a (very) strong emotional impact, while 16% remain relatively unaffected.

In the aftermath of scams, Australians grapple with complexity, attempting to decipher deceit and lacking the digital savviness to outsmart modern-day cyber threats. Common scam checks, such as "if it's too good to be true, it probably is," echo in the digital landscape, but not all navigate this intricate dance with finesse.

A groundbreaking initiative emerges from the heart of the Anti-Scam Center, charting a bold course to transform the landscape. The mission ahead is clear: to weave a robust shield against the looming threat of scams that plague our digital realms. Propelling this mission is the call for comprehensive and binding cross-industry standards, transcending traditional boundaries to encompass banks, telecommunications, digital platforms, and cryptocurrency exchanges. This visionary approach not only safeguards financial institutions but also heralds a new era of resilience in the face of evolving scams. The journey forward hinges on collaborative alliances with key stakeholders, creating a united front against the intricate web of fraudulent activities. It's a narrative of innovation, solidarity, and the collective pursuit of a scam-resistant future.

In conclusion, the 2023 State of Scams in Australia report isn't just a data dump; it's a call to arms. Aussies, known for their resilience, larrikin spirit, and knack for a fair go, are summoned to elevate digital defenses, sharpen their scam detection prowess, and streamline reporting mechanisms. It's time for Australians to unite in the digital frontier, turning the page on the digital saga, and crafting a narrative where they emerge victorious against the rising tide of online deception. The stage is set, and the sunburnt land awaits its digital champions.

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

Working together to end the scams contagion

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 75% of Australians experience a scam on a monthly basis. Unfortunately, 61% of Australians don't report scams to law enforcement because 1) they are uncertain where to report it, or 2) they don't think it'll make a difference. About 54% of Australians turn to their bank when they fall victim to scams, while only 28% report it to their local police department. 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.

At the end of 2023, Australian banks joined forces to launch The Scam-Safe Accord. This decisive and robust offense against scammers signal a significant shift and commitment in the banking industry's approach to stronger fraud prevention. Central to the effort to reduce scams is a $100 million investment in a new "confirmation of payee" (CoP) system. CoP involves a thorough check to ensure that money transfers align with the intended recipient's details. With over 15.4 billion transactions annually, implementing this system across the banking sector is a monumental task set to unfold between 2024 and 2025.

This is an inspiring step in the collaborative approach to enhance the fight against scams. Banks, 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.

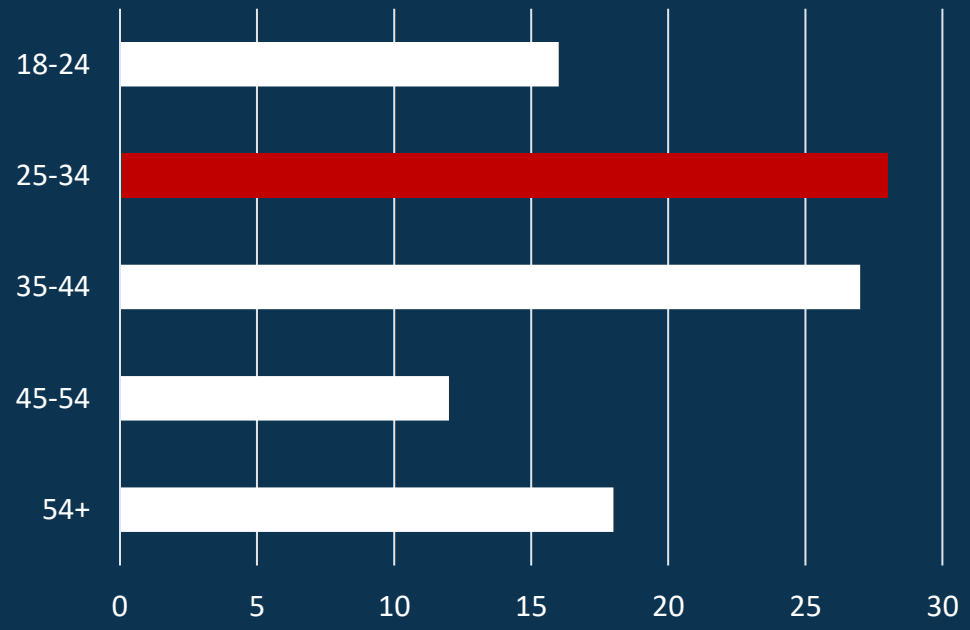
Feedzai is a proud partner of GASA and aims to equip financial institutions with the tools they need to prevent scams and protect consumers. Learn more about Feedzai here.

David Haynes
Vice President and General Manager of Asia Pacific
Feedzai

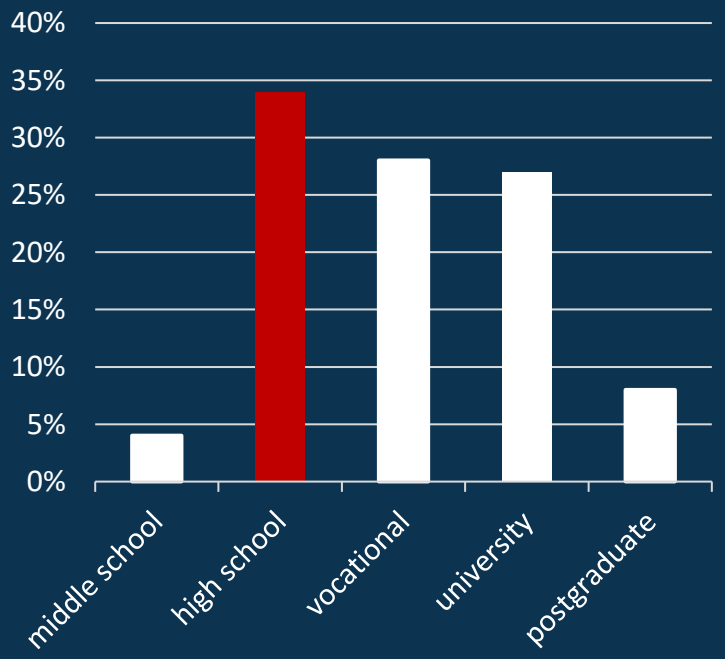
1,000 Australians participated in the survey

Gender

Age

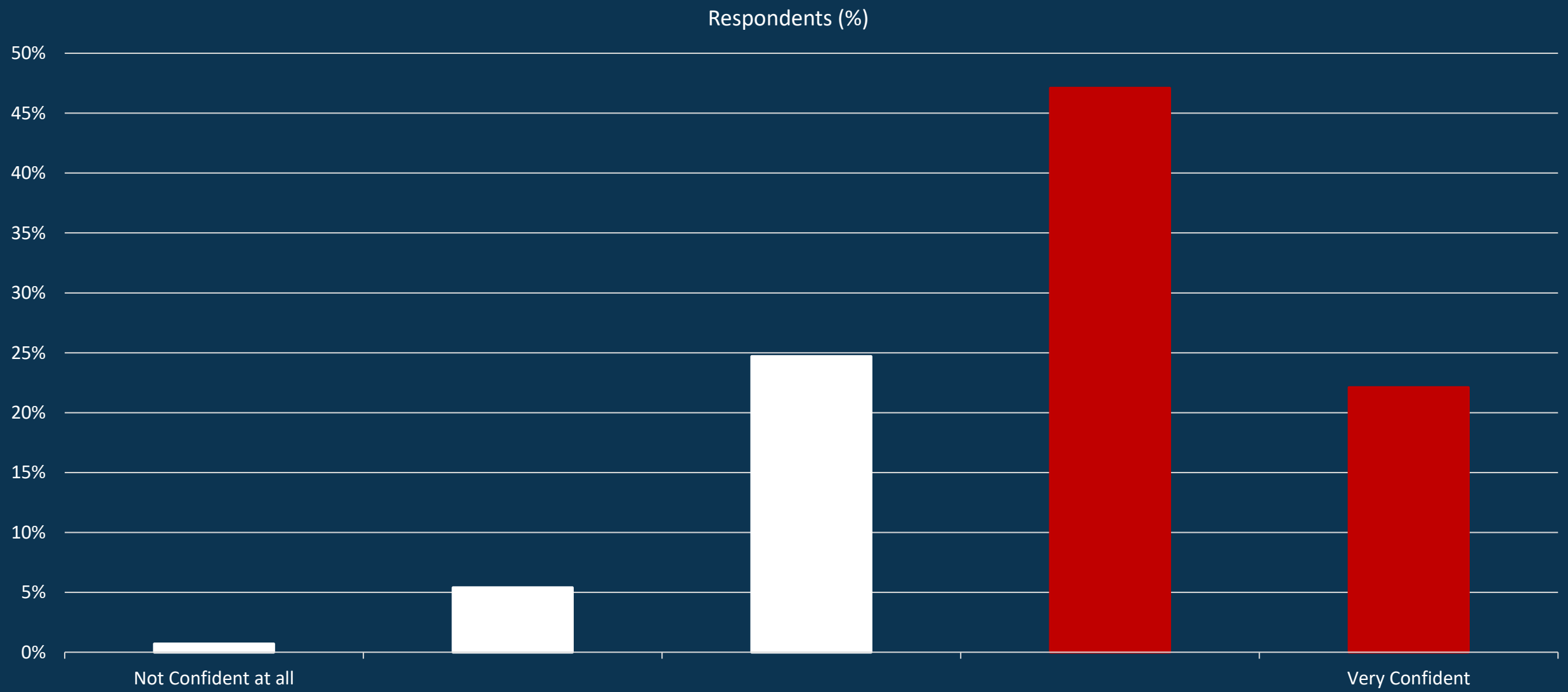


Education



More women than men participated, mainly in the age groups 25 – 34 with High School education.

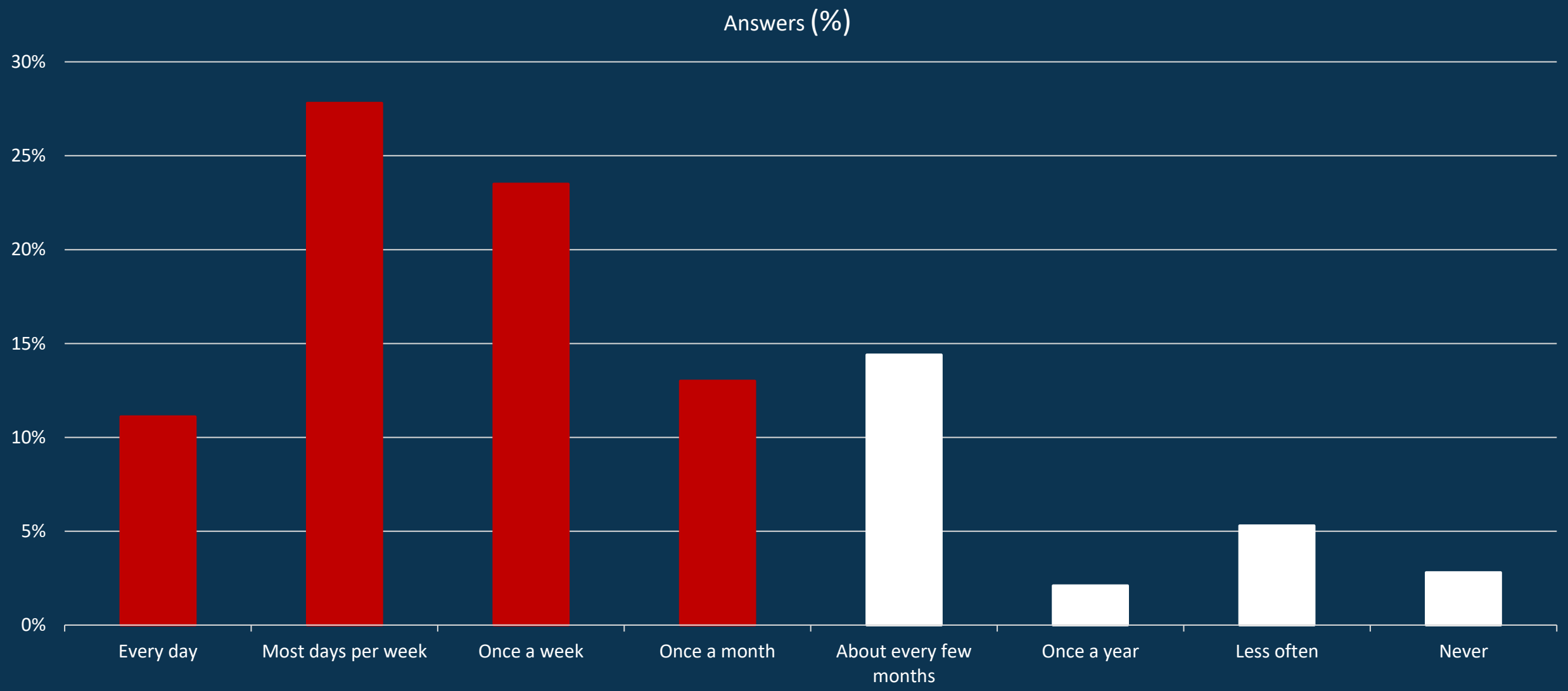
69% of Australians are (very) confident that they can recognize scams



Only 6% is not (very) confident at all.

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

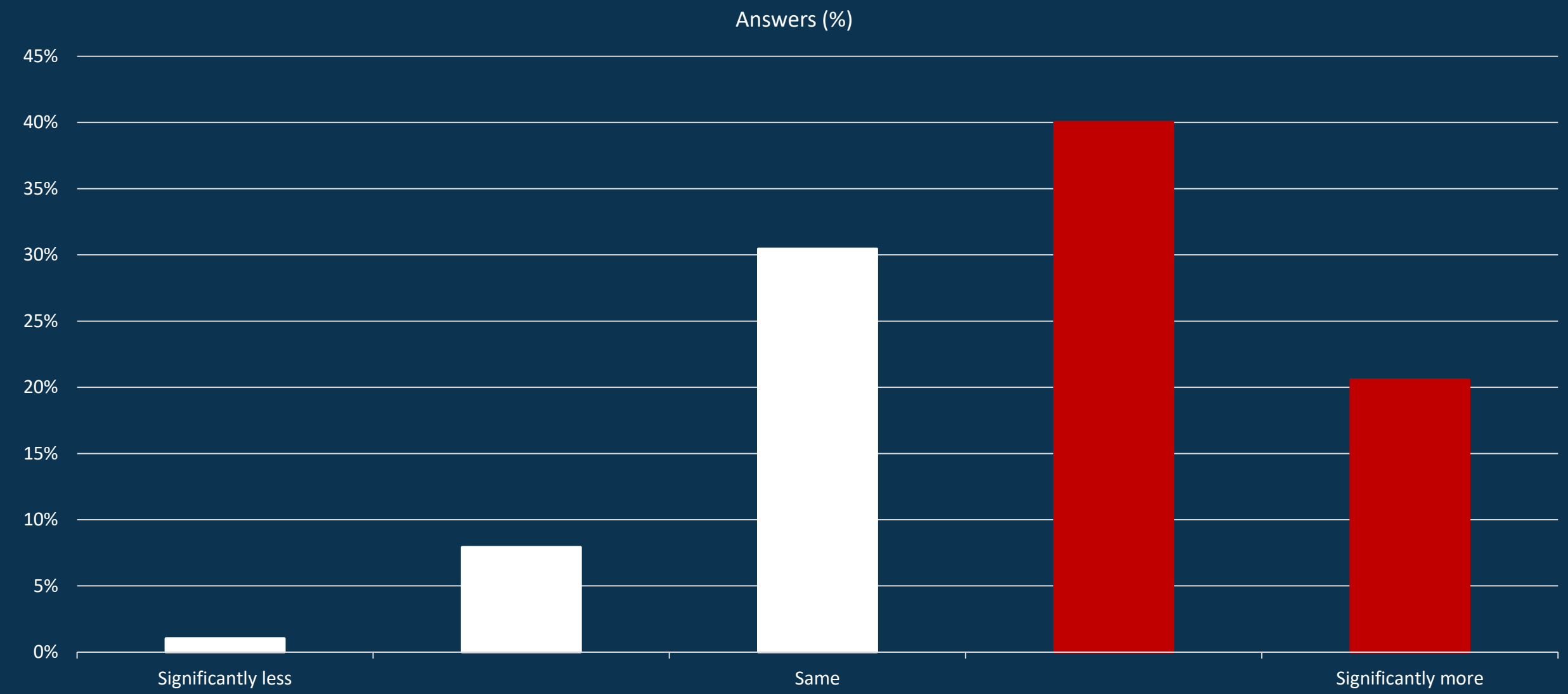
75% of the Australians encounter a scam at least once per month



14% 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)?

61% of Australians experienced more scams in the last 12 months



Only 9% 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?

Australia Fights Back with National Anti-Scam Centre & Cross-Industry Standards

In Australia, the fight against scams is in full swing, as government and industry coordinate efforts to curb the menace and protect citizens from predatory tactics. In the Australian report on scams, we bring to you insights from Heidi Snell, the Executive General Manager of the National Anti-Scam Centre at the Australian Competition & Consumer Commission (ACCC). Here, she explains the current state of scams in Australia, the trends in 2022, and the government's robust strategy to tackle this issue head-on.

Can you give an overview of the extent of scams in Australia according to recent data and the effects on victims? Absolutely. The 14th annual Targeting Scams report by the ACCC highlighted that in 2022, scams accounted for over $3.1 billion in losses. The figures have been rising steadily since 2020, with Scamwatch recording $569 million in losses last year, a stark 80% rise from 2021. Unfortunately, this year we have already witnessed a 44% surge in reports, with losses approximating $351 million. The repercussions for victims are substantial, with the average loss in 2022 soaring by 54% to nearly $20,000, resulting in a long and difficult recovery process.

Which scams stood out the last year in your country and were "trendy"? Last year, ***investment scams*** were predominant, particularly those facilitated via phone and social media, with cryptocurrency being the common payment medium. ***Bank impersonation scams*** were also rampant with 14,603 reported cases, where scammers would pretend to be calling from a bank's cybersecurity or fraud department. ***Employment scams*** have risen substantially, with scammers exploiting social media to offer faux work-from-home opportunities, usually associating themselves with legitimate companies and promising substantial earnings for minimal effort. Furthermore, ***impersonation websites*** mimicking renowned retail brands emerged to trick consumers into revealing their credit card details or paying for undelivered goods. In terms of scam contact methods, ***text messages*** surpassed phone calls as the primary contact method, registering an 18.8% increase on the previous year.

Which actions have been taken by your government and other organizations to protect consumers from scams? Any best practices from which we can learn? To counter the increase in sophistication of scams, the Australian government establish the National Anti-Scam Centre on 1st July 2023 focusing on a whole of ecosystem approach to scam prevention and detection. It brings together government and private sectors to thwart scams through data & intelligence gathering, disruption through fusion cells, and enhancing public awareness and education. Australia has implemented codes to minimize scam calls & messages and is developing a registry to block scam texts impersonating well-known organizations. Some parts of the financial sector introduced initiatives such as payment delays, name & account matching, blocking high-risk crypto platforms and real-time scam account data sharing.

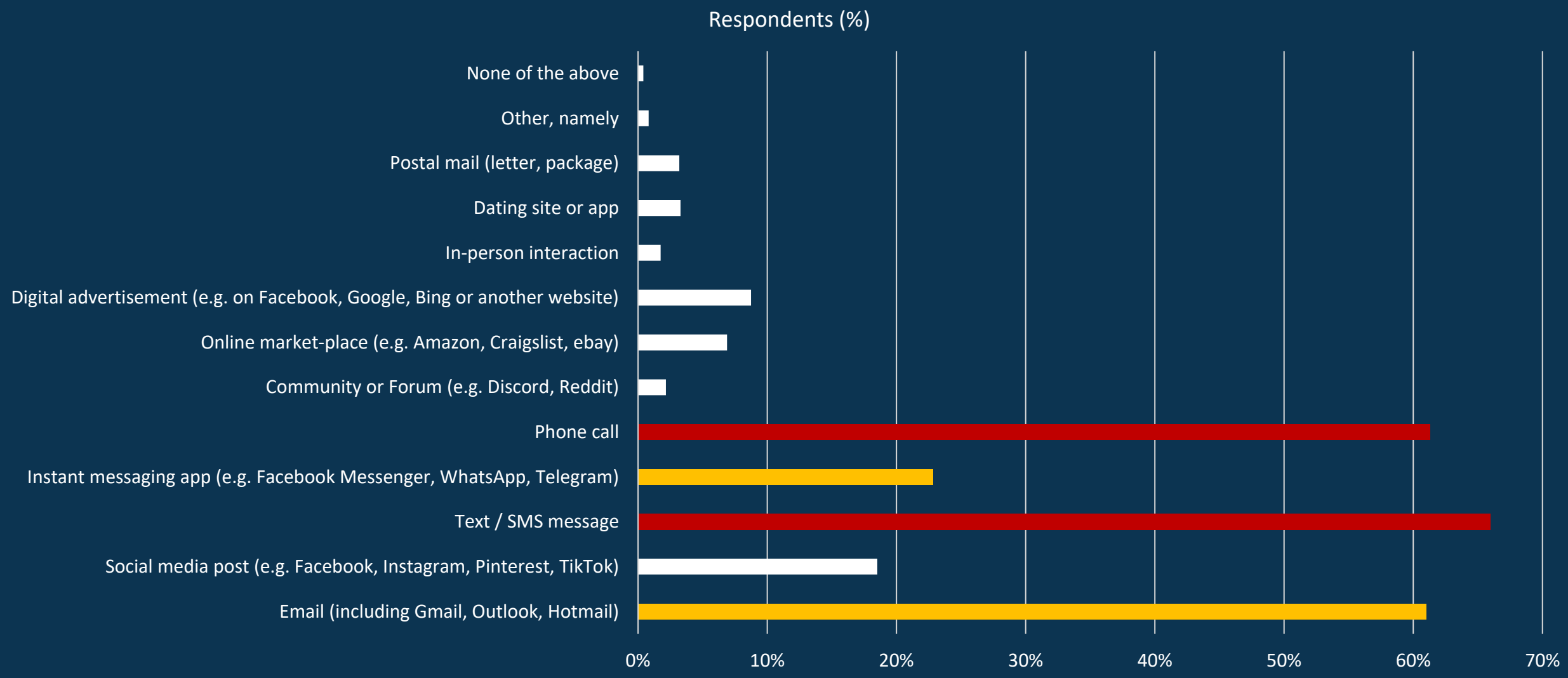
What further initiatives do you propose to empower consumers in their fight against scams? Moving forward, we aim to bridge the existing gaps in the ecosystem that make it susceptible to scams. We advocate for the establishment of mandatory and enforceable cross-industry standards that encompass not just banks but also telecommunications, digital platforms, and cryptocurrency exchanges. Collaborative efforts with relevant stakeholders will be pivotal in building a scam-resilient ecosystem.

With cohesive efforts from government and private sectors, Australia aims to cement a resilient digital ecosystem, safeguarding its citizens from scams. Heidi Snell's insights reflect a steadfast pledge to adapt, take action, and to ensure Australians look forward to an increase in security and prosperity.

Heidi Snell
Executive General Manager
National Anti-Scam Centre at the Australian Competition & Consumer Commission

Australian Government | National Anti-Scam Centre

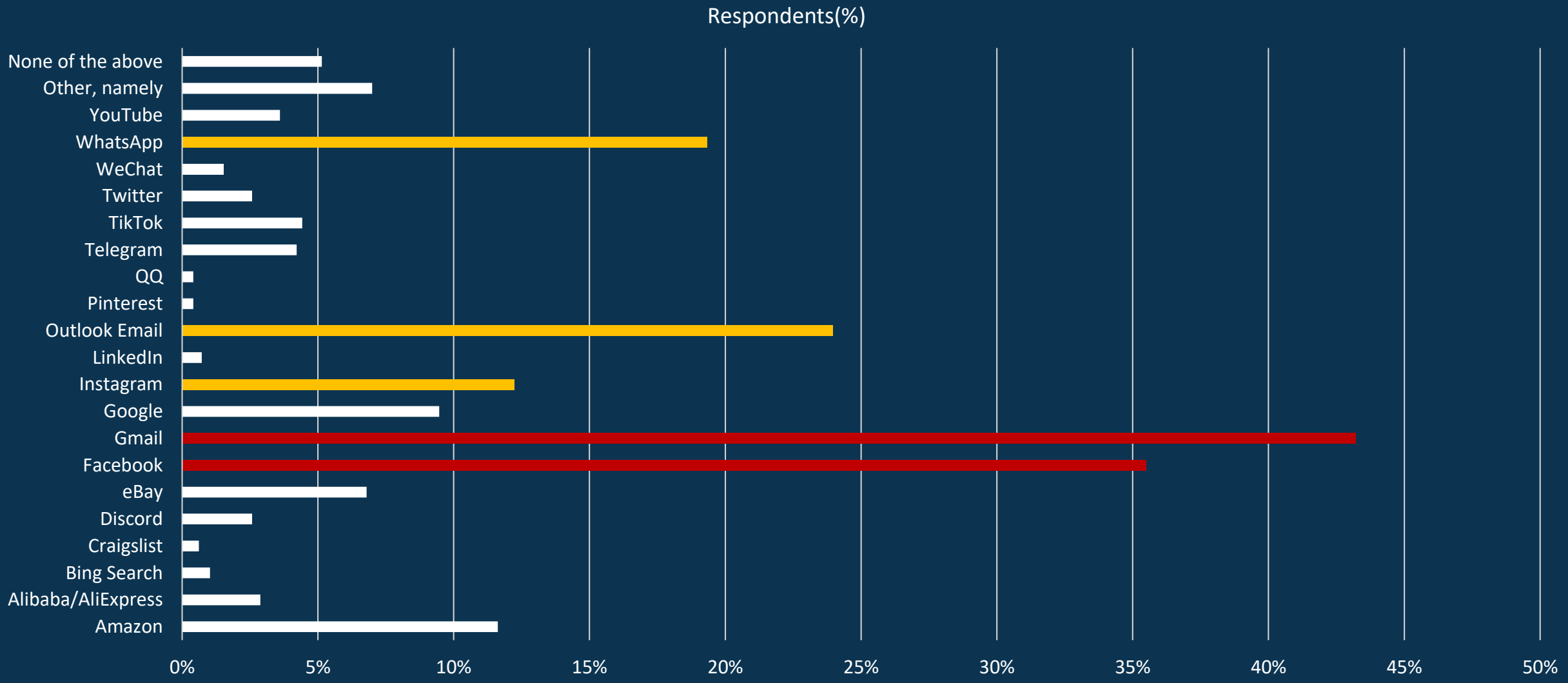
Most Australians receive scams via Text/SMS Messages and Phone Calls



However, Emails and Instant Messaging Apps are also very 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.

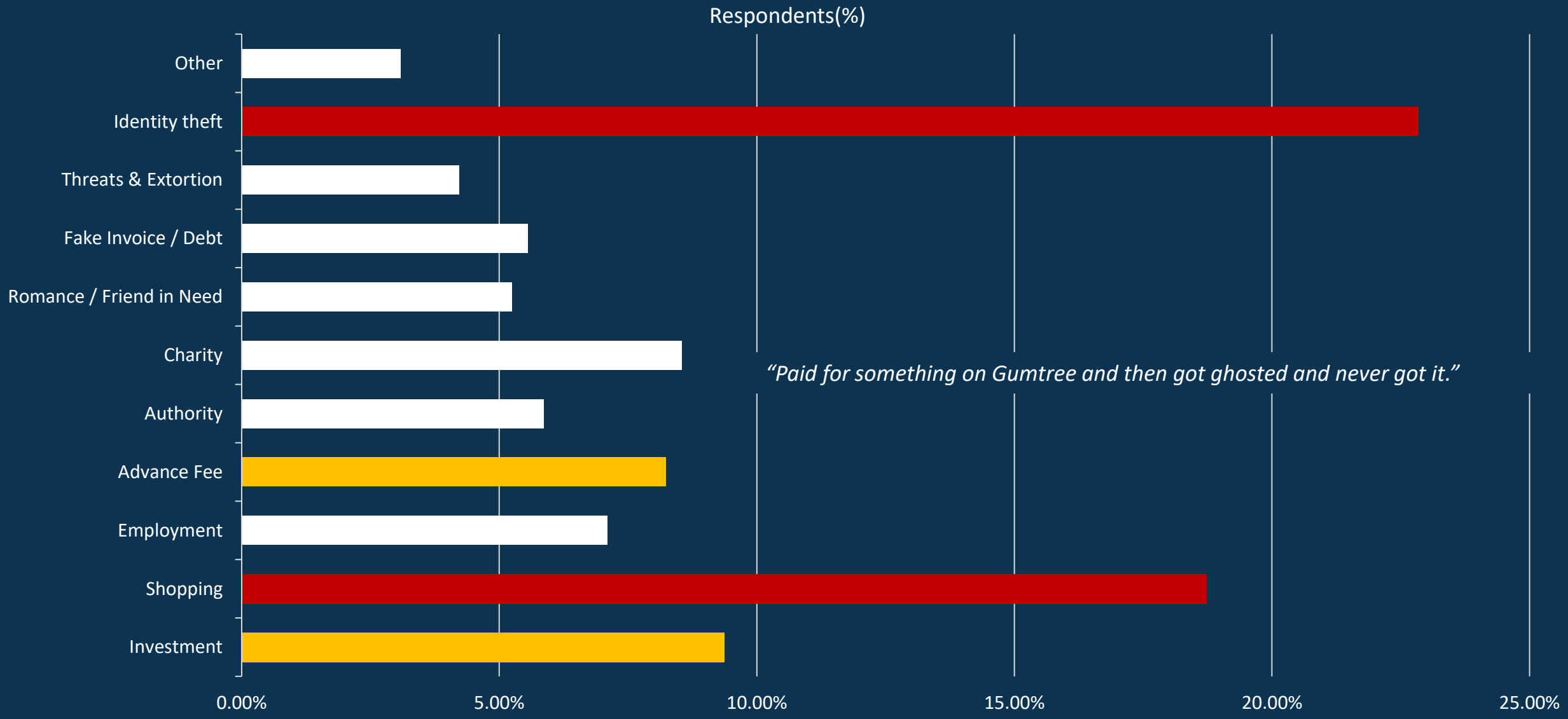
Gmail and Facebook are the platforms most exploited by scammers



Outlook Email, WhatsApp and Instagram take 3rd and 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 type of scam in Australia



"Paid for something on Gumtree and then got ghosted and never got it."

45% stated they had not fallen victim to the most common scams in the last 12 months. 1.76 scams were reported per scam

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

Scams are hurting Australians in many ways

“My personal information including card details were accessed and my bank account was debited a substantial amount of money. I had to cancel the card and report it, the bank reimbursed the money to me.”

“I was apparently awarded a $750 Shein giftcard, but after completing a couple "deals", $89 was taken from my bank account. They were called “Smartarn" on my account statement.”

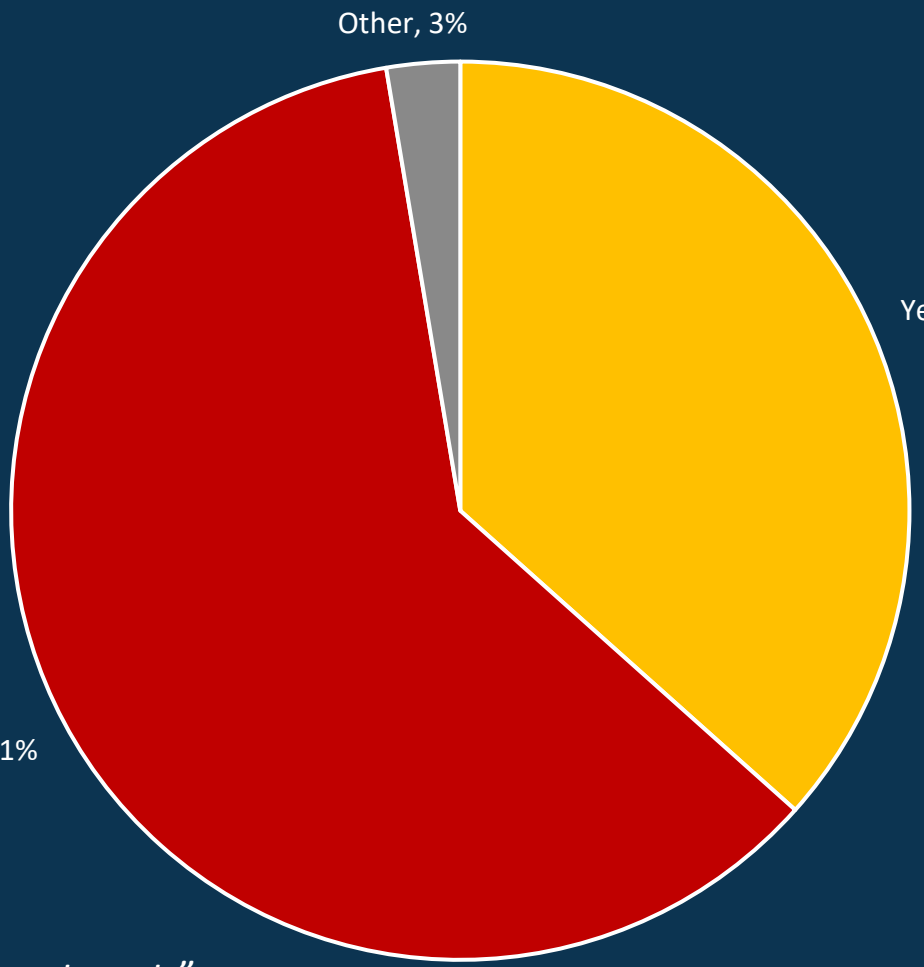
“The program promised to give steady returns from matrix system, but no one got any money as the program disappeared after few months.”

“I tried to purchase a brooch as a Christmas present from an online store. I never received the brooch. I tried contacting the company numerous times and they never responded.”

“Someone on a community Facebook group claimed to be desperate for groceries. I sent her money because i didn’t have time to go to the shops and drop off to her. I later find out from the admin that she goes from group to group asking for the same thing.”

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

61% did not report the scam to law enforcement



"I complained to eBay regarding the scam and requested a refund."

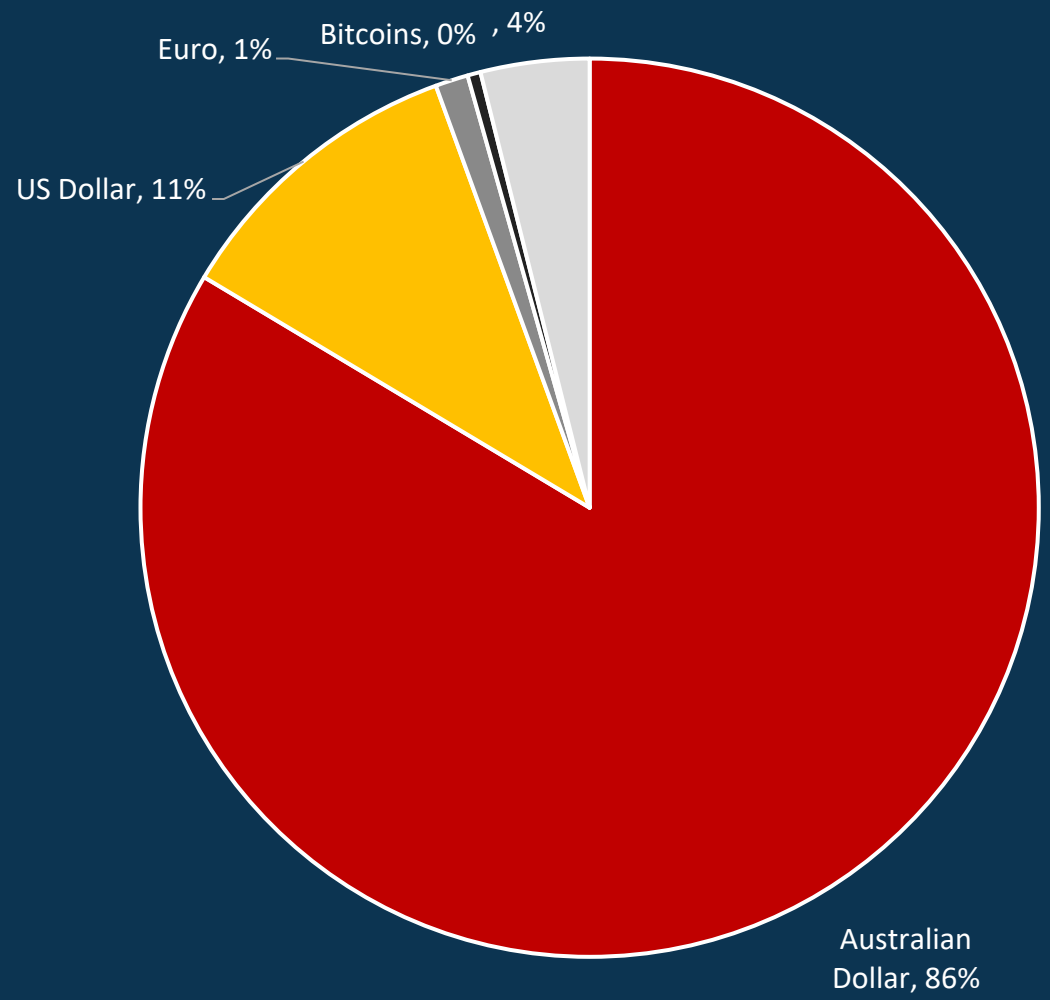
"I reported the scam to my banks fraud department."

37% 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 17% of the approached persons reported losing money in a scam

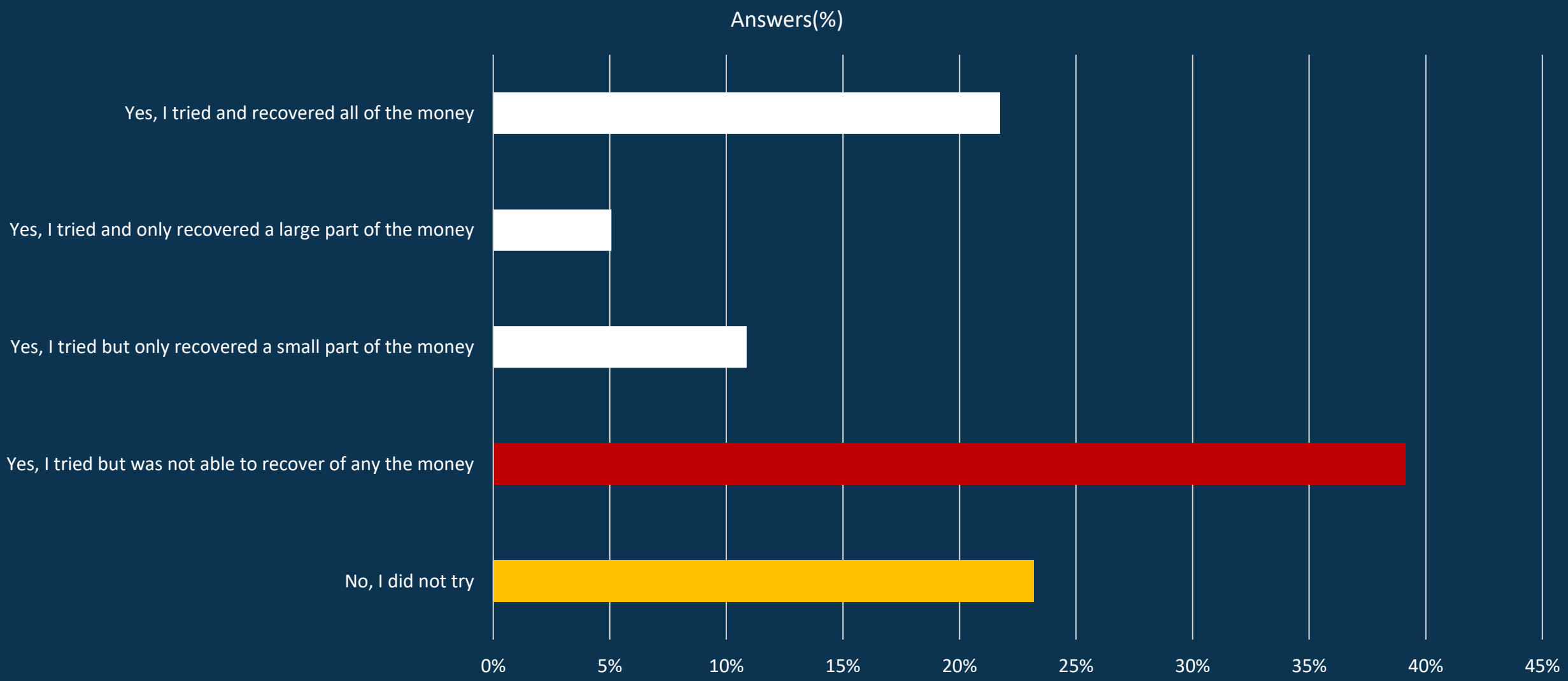
Survey Key Statistics	
Number of persons approached	2369
Participants completing the survey	47%
Participants losing money	414
% losing money / approached persons	17%
Average amount lost in US Dollars	$1,548
Total country population	26,461,166
Population over 18 years	20,608,845
# of people scammed > 18 years	3,601,546
Total amount lost in scams*	$5,575,192,787
Gross Domestic Product ($ millions)	1,707,548
% of GDP lost in scams	0.3%



Most scams were reported in Australian Dollars (86%), the remainder is mainly in US Dollars (11%) and a few Euros.

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".

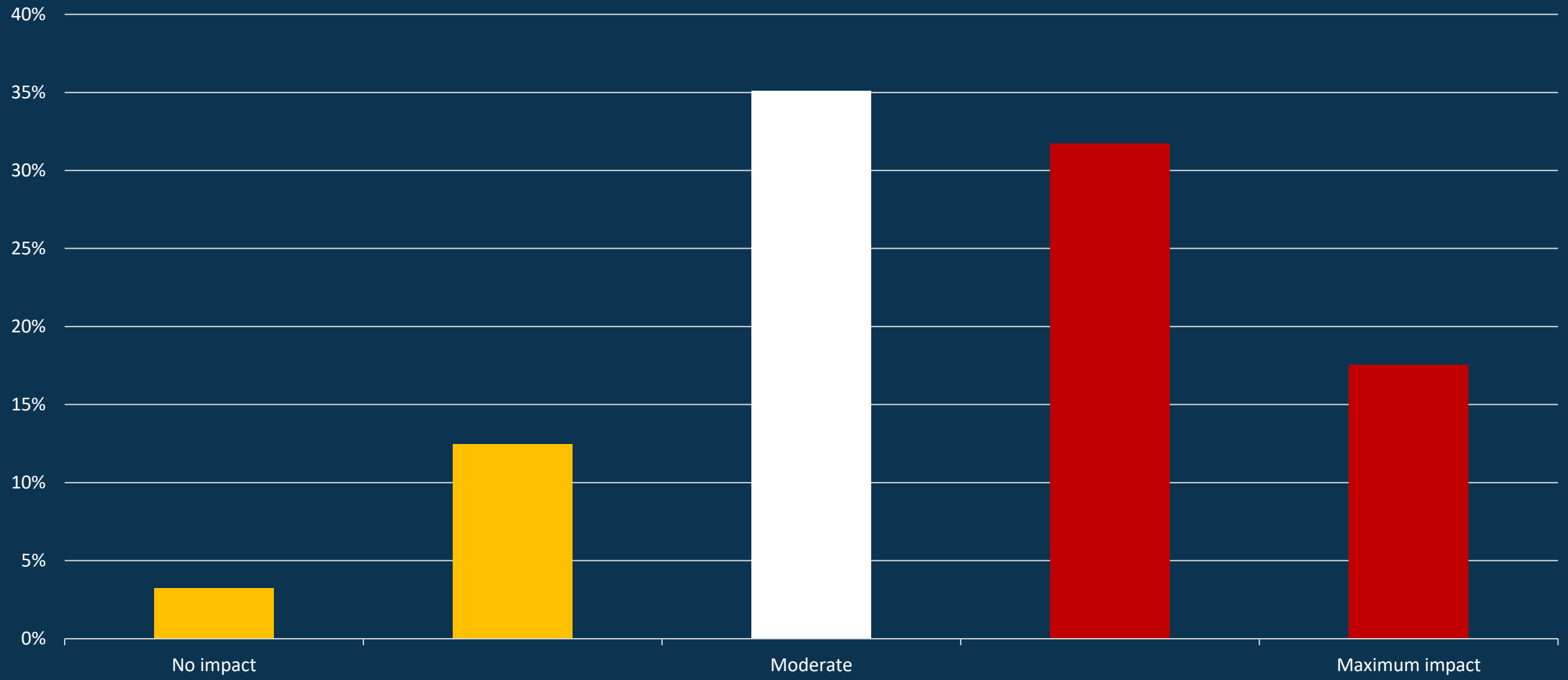
Only 22% of the survey participants were able to completely recoup their losses



23% did not try to recover their funds. 39% tried but were not able to recover any money.

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

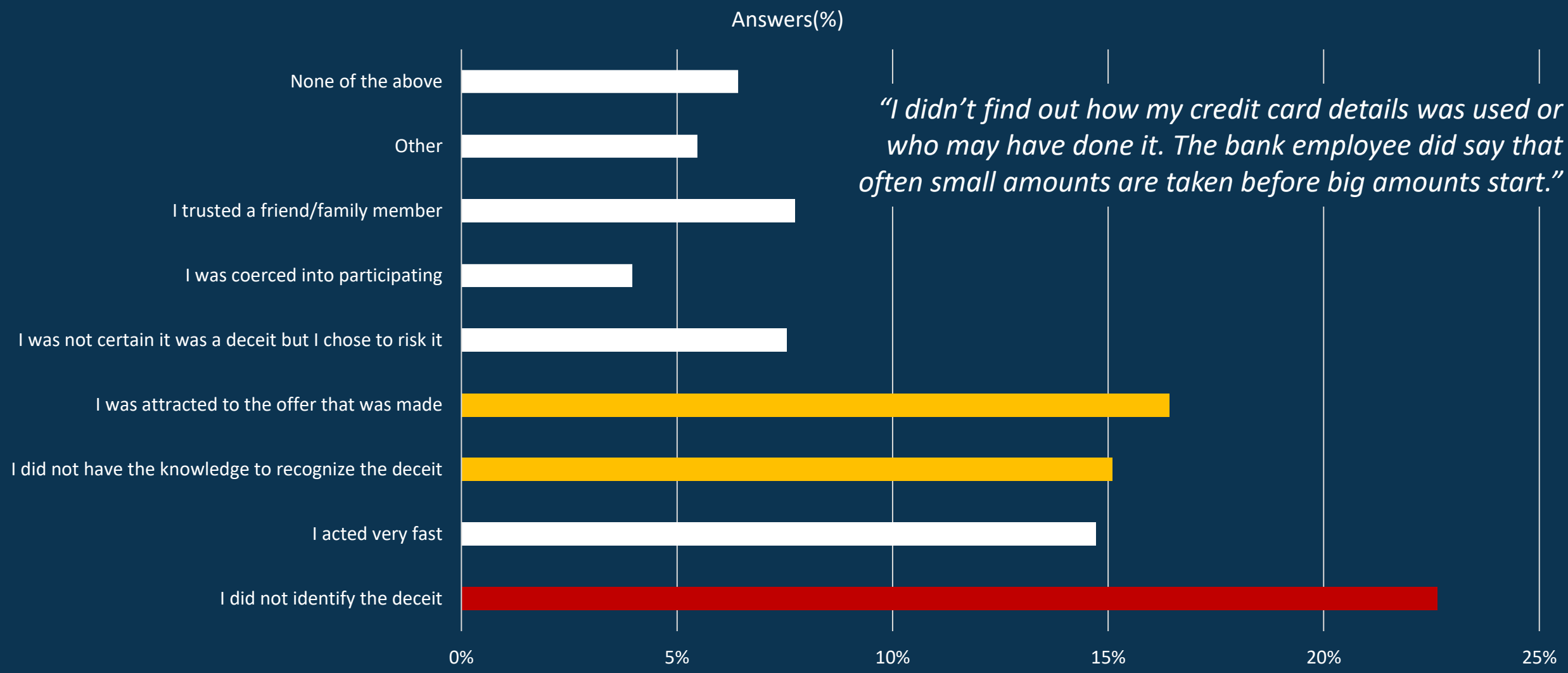
49% of the scam victims perceived a (very) strong emotional impact



16% 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 Australians fall for a scam is their inability to identify deceit

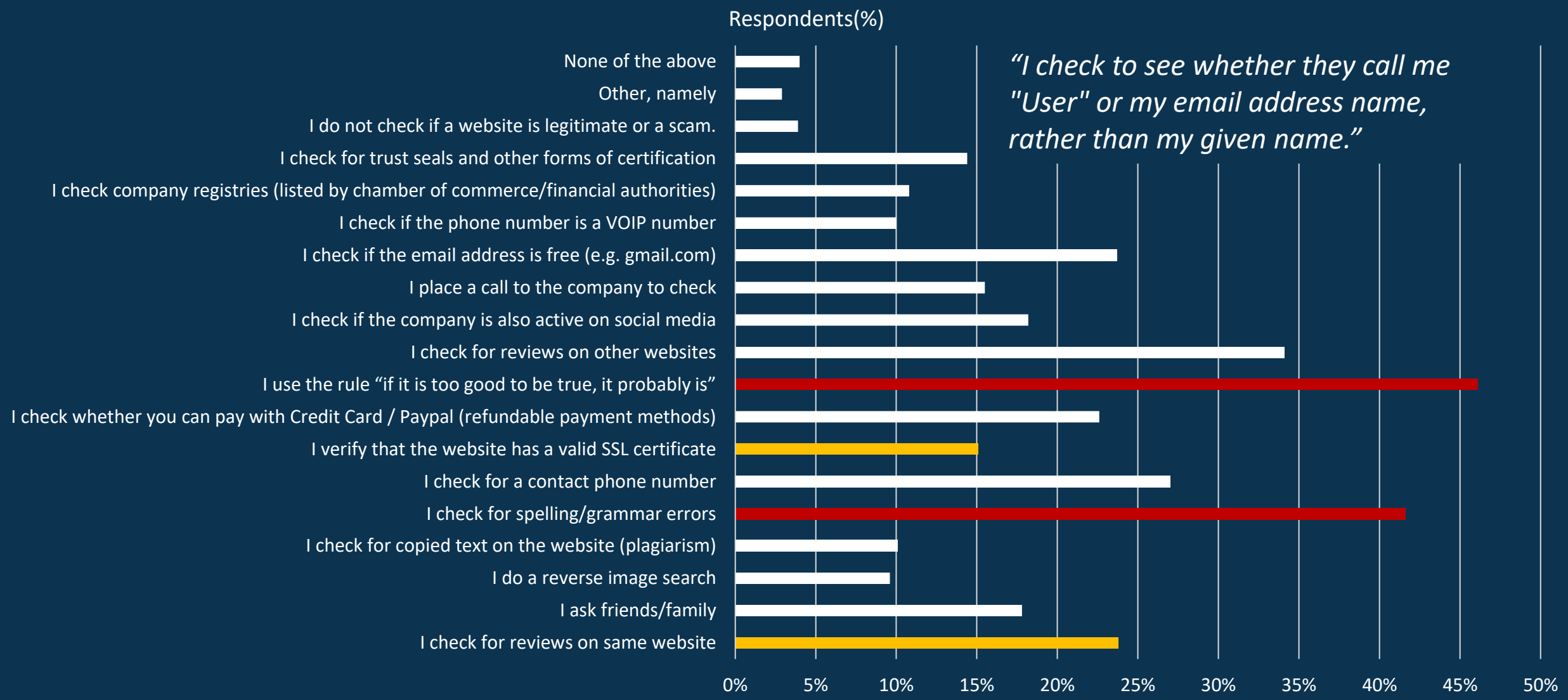


"I didn't find out how my credit card details was used or who may have done it. The bank employee did say that often small amounts are taken before big amounts start."

Several victims also reported being caught out by the offer made while others didn't have the knowledge to recognize deceit.

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

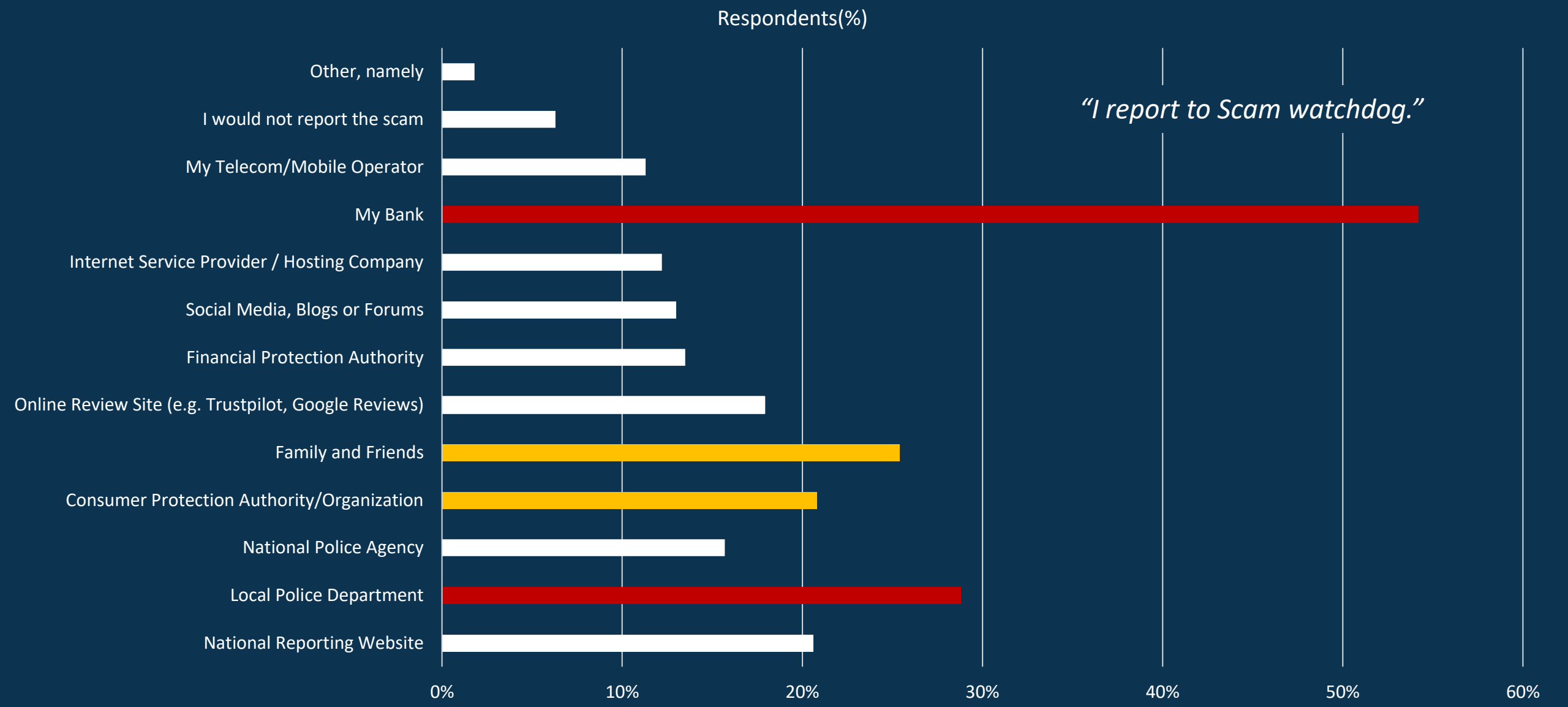
The most common scam check is “if it is too good to be true, it probably is”



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.

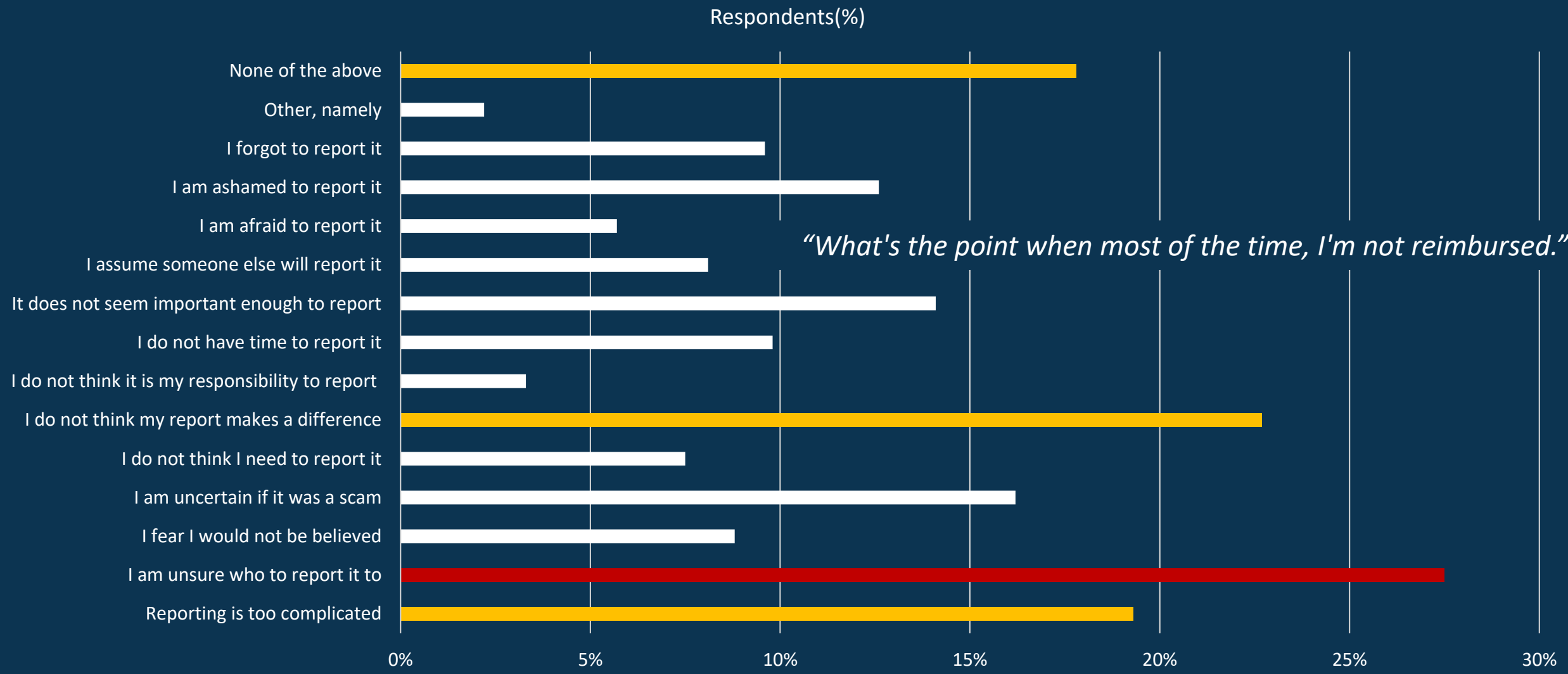
Scams are mostly shared with Banks and Local Police Department



Family & Friends and Consumer Protection Authority are popular scam reporting destinations.

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

Most Australians are uncertain about where to report scams

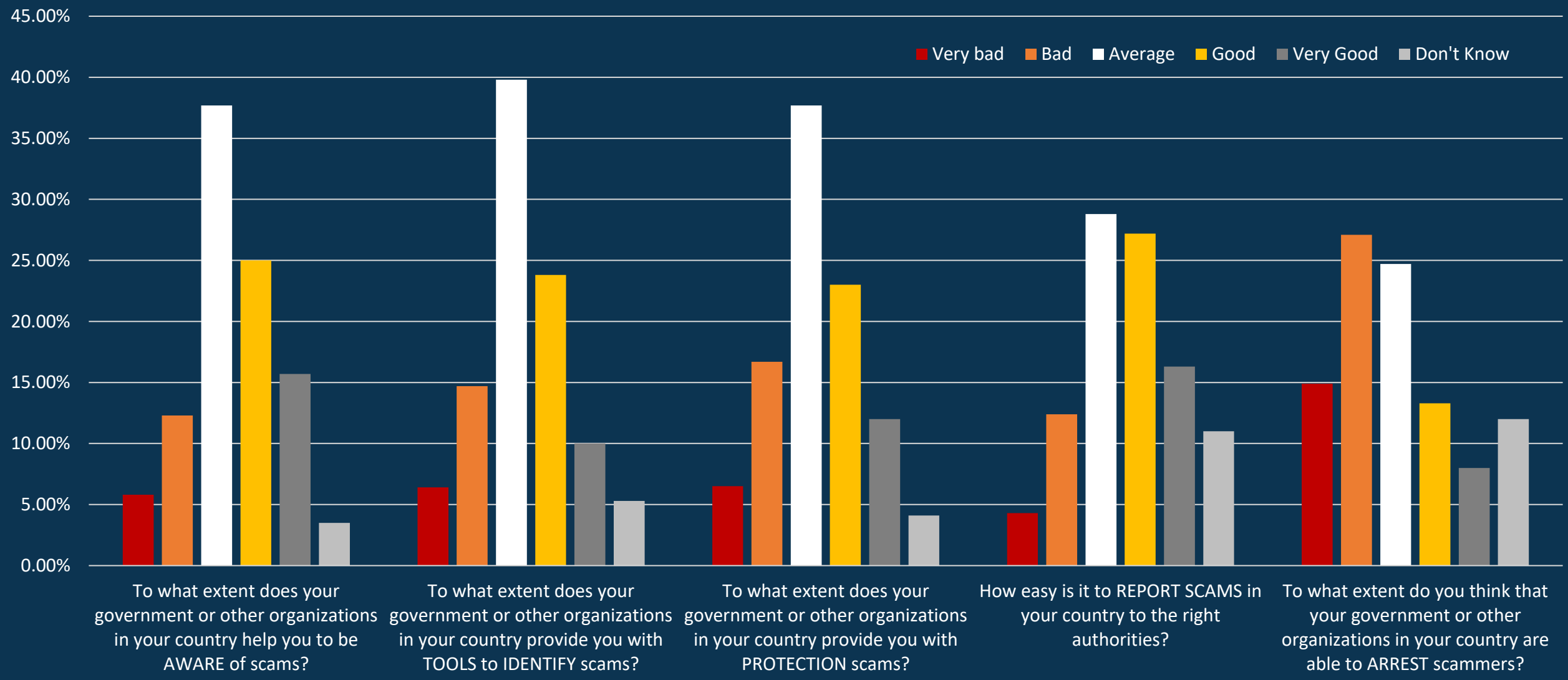


"What's the point when most of the time, I'm not reimbursed."

Other key reasons for not reporting are assuming reporting won't make a difference and complex reporting process.

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

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



Overall, 24% of the participants rate the actions of governments as (very) bad, 35% 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

“Those investment programs are out of my country, most of them provide London address, but they operate from other countries that it's hard to get any action from authorities.

“I was scammed on Facebook. I reported it to Facebook, and nothing was done. The same was sponsored so I just don't buy anything advertised on Facebook.”

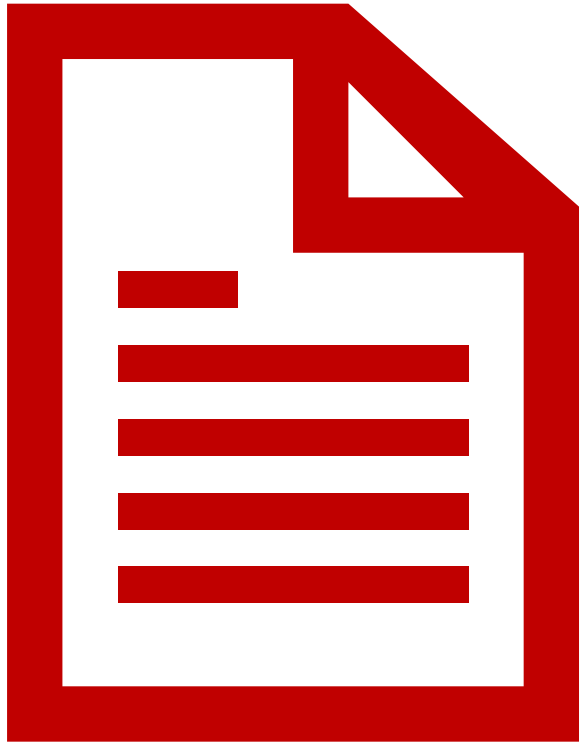
“I no longer accept phone calls where a don't recognize the number calling. I very rarely click on links in SMS or text messages unless it is one I have done so many times in the past.”

“The government should introduce harsh penalties for social media platforms that perpetuate scams.”

“I really do think the government should take scams for seriously and re-educate the topic in high school and possibly universities.”

feedzai

About this Report



GASA
Global Anti-Scam Alliance

Who are we?

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.

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.

Copyright

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