



The State of Scams In New Zealand - 2023

17% of Kiwis lose money as scammers make off with NZ\$2.05 billion

In an age where our digital footprints touch almost every aspect of our lives, ensuring the safety and security of individuals and their personal data has never been more paramount. It is with a shared vision and collective responsibility that the Global Anti-Scam Alliance and Netsafe New Zealand come together to address one of the most pressing challenges of our time – scams.

Both our organizations understand the profound impact of scams on individuals, families, and communities. Beyond the financial repercussions, scams erode trust, inflict emotional trauma, and undermine the very fabric of our digital society. Recognizing the urgency of this issue in New Zealand, we have joined forces, leveraging our combined expertise, research capabilities, and outreach networks to present this comprehensive report.

Through this collaborative endeavour, our aim is clear: to educate, inform, and empower every Kiwi, ensuring they have the knowledge and tools to safeguard themselves against the myriad of scams that continue to evolve in complexity and cunning.

A thousand Kiwis eagerly responded to our survey, revealing a daunting landscape of deception in New Zealand. Notably, the majority of our participants were women from the age group 25-34, boasting high school and university education. With 68% expressing confidence in recognizing scams, it's unsettling to learn that 62% still encounter these tricks at least once a month. Over half witnessed a rise in scams over the past year, emphasizing the growing threat.

Scammers tailor their tactics to the Kiwi digital landscape. Platforms like Gmail (43%) and Facebook (37%) are primary hunting grounds. Identity theft emerged as the paramount concern, haunting 20% of our respondents. Tales of online shopping mishaps, unauthorized credit card transactions, and counterfeit charity fronts abound. Scams are not just a financial threat but a deep emotional strain as well. "The 'cancer society' scam," as one respondent recounted, "was a jarring experience, realizing I had been duped by a fake charity."

This dark cloud isn't without its silver lining. Kiwis employ strategies like checking if an offer is "too good to be true" to safeguard themselves. Banks and the New Zealand Police remain the primary entities to report these deceitful tactics. Still, many hesitate, doubting the effectiveness of reporting. In fact, a significant 59% didn't report the scam they faced, echoing a sentiment of resignation rather than resistance. Only 35% turned to law enforcement or other governmental agencies.

The numbers further tell a tale of loss and caution. Of the participants, 17% lost money to scams, with an average loss of NZ\$3,165 (US\$1,846), amounting to a staggering NZ\$2.05 billion (US\$1.2 billion) lost nationally. It's alarming to note that scams account for 0.5% of New Zealand's GDP, highlighting a pressing concern for the nation's economic health.

Recovery tales are few and far between, with a mere 15% managing to reclaim all their lost funds. The emotional toll is evident, with 53% admitting to a significant emotional impact post scam.

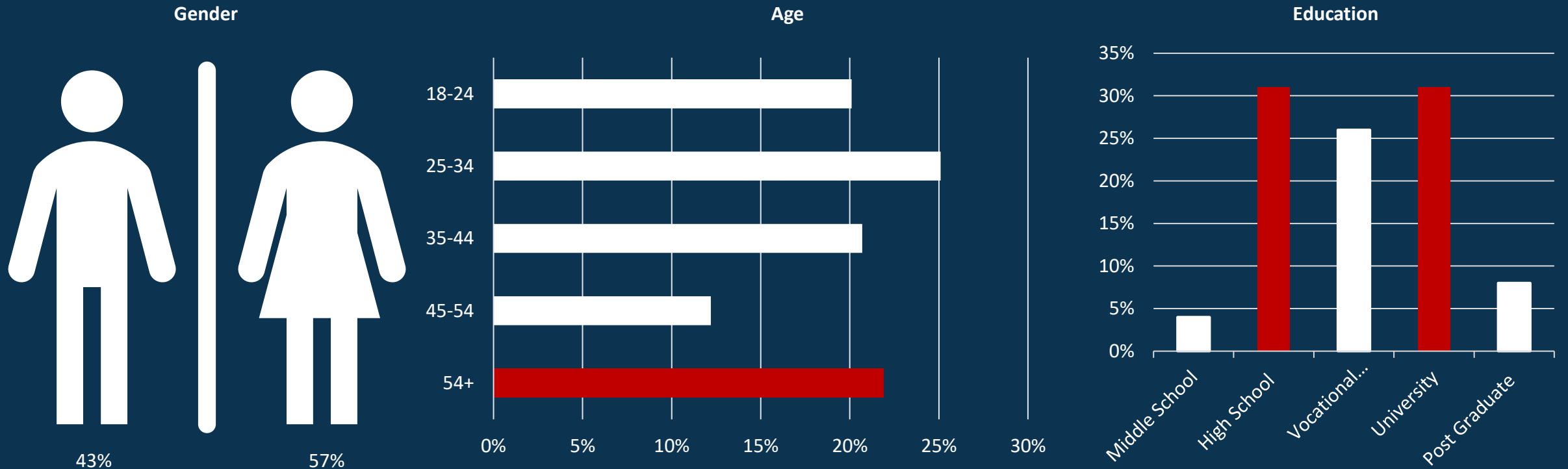
Trust in governmental intervention hangs in the balance. 24% rate their government's efforts to combat scams as unsatisfactory, but a significant 33% laud it as commendable. Calls for better security echo through the accounts of many, with a need for more clarity on reporting procedures and swifter action against scammers.

The modern Kiwi battles not only the natural challenges of their beautiful nation but also the digital pitfalls of the 21st century. Scams, evolving in complexity and frequency, remain a significant concern, and New Zealand, like many countries globally, stands at the forefront, seeking ways to combat this menace. We call upon every New Zealander to join us in this mission, to share this knowledge, and to stand together in our fight against scams. As a cohesive and informed community, we can create a safer, scam-resilient digital New Zealand.

Jorij Abraham, Managing Director, Global Anti-Scam Alliance

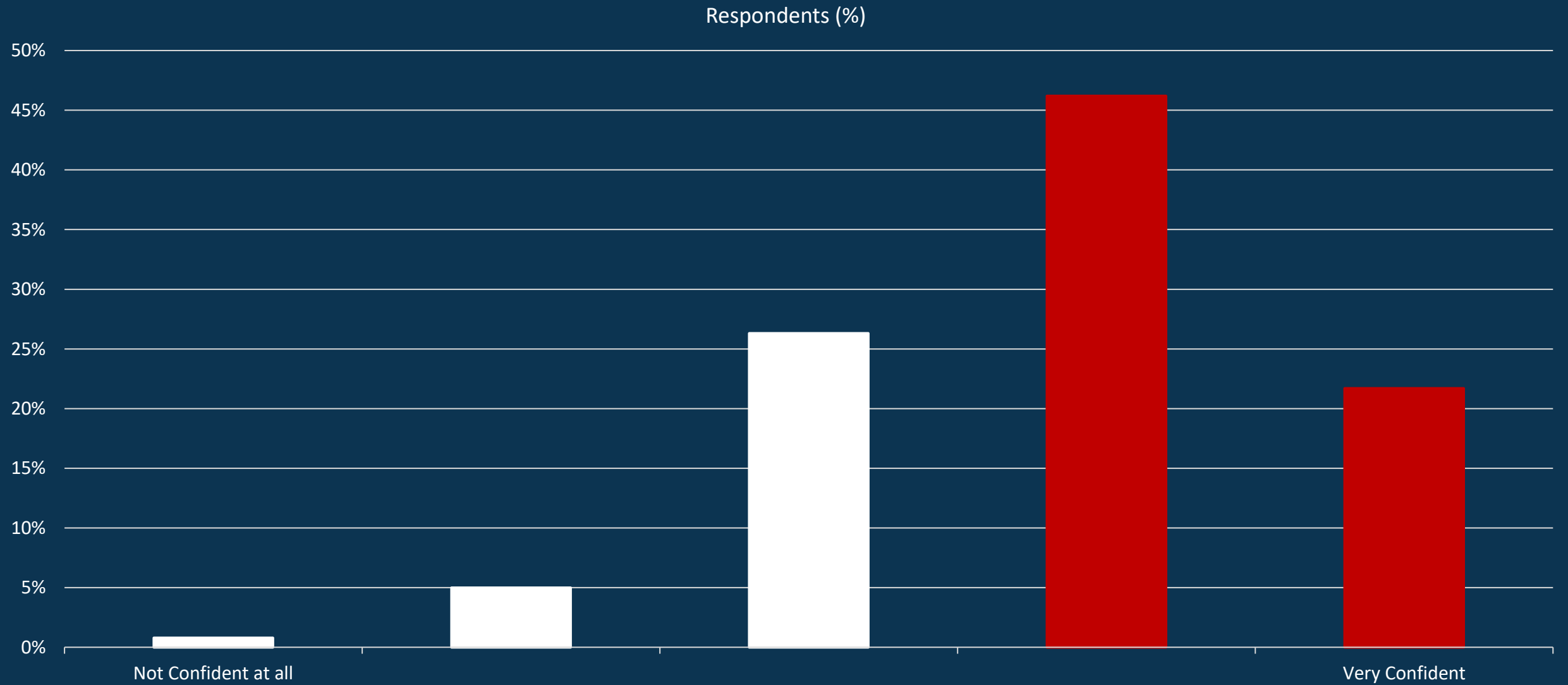


1,000 Kiwis participated in the survey



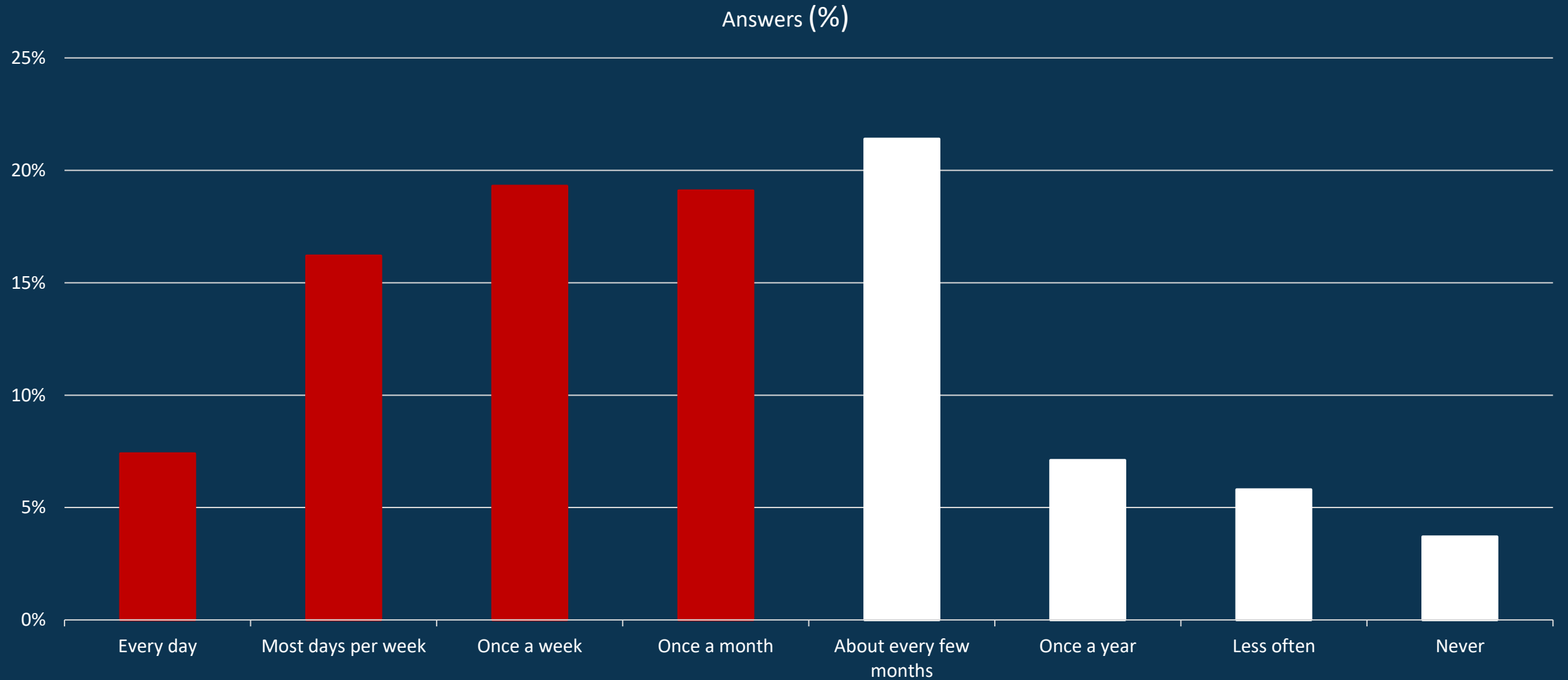
More women participated than men, mainly in the age group 25 – 34, with a high school education or university degree.

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



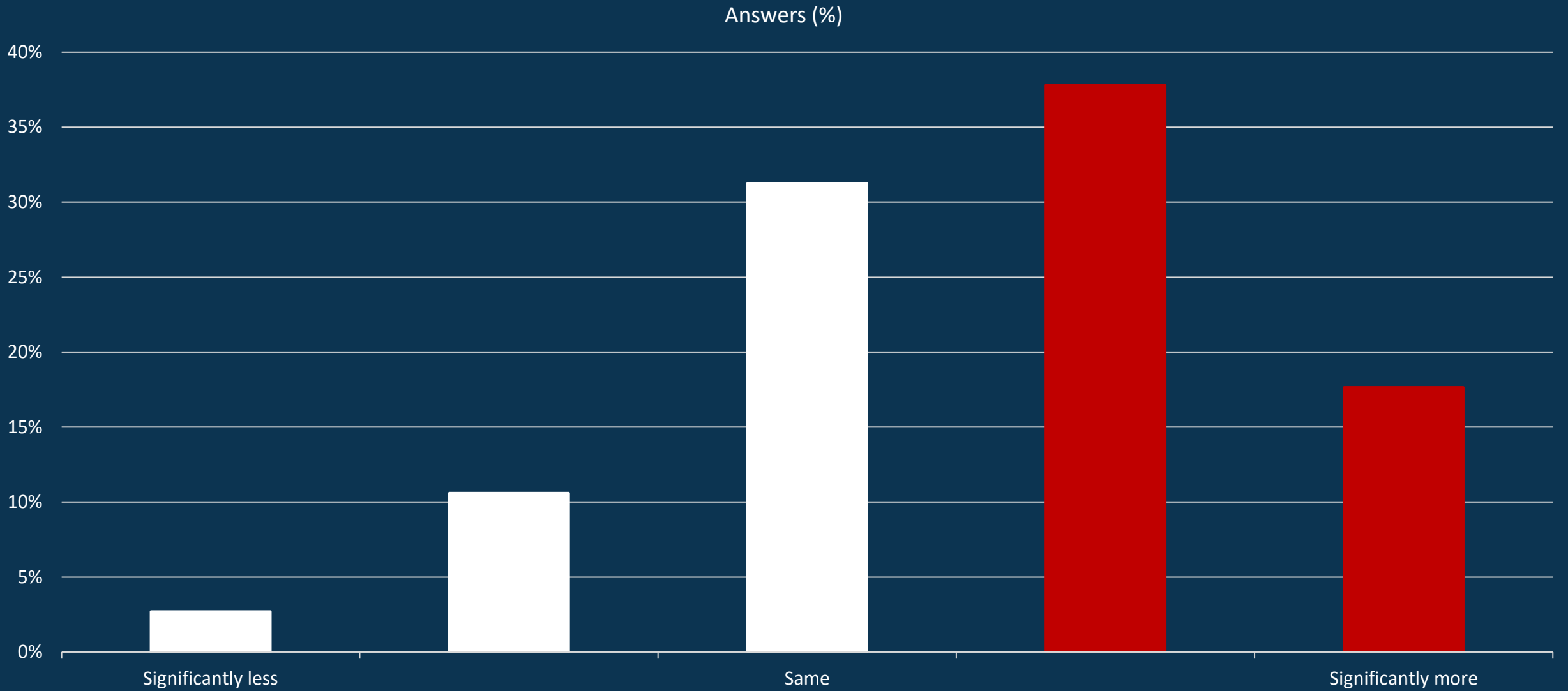
6% are not (very) confident at all.

62% of the Kiwis encounter a scam at least once per month



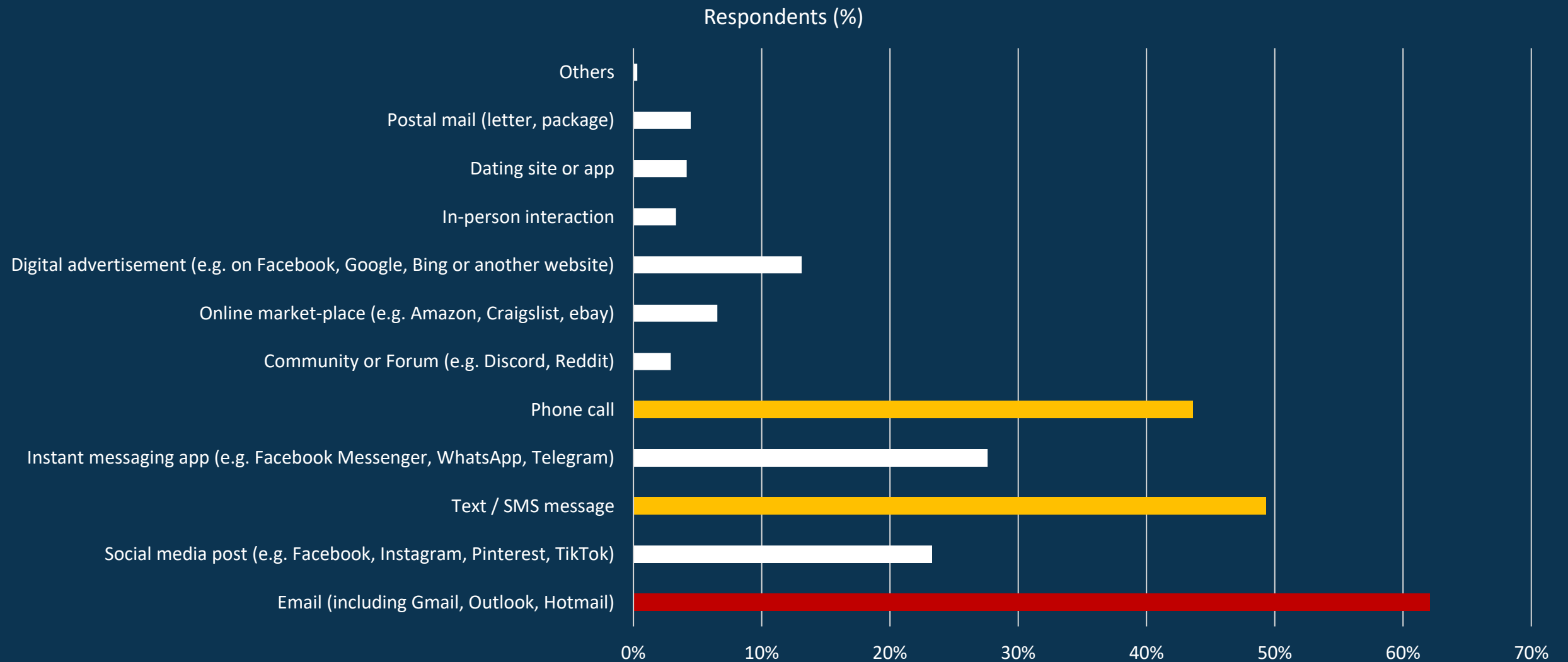
21% experience a scam (attempt) at least every few months.

55% of Kiwis experienced more scams in the last 12 months



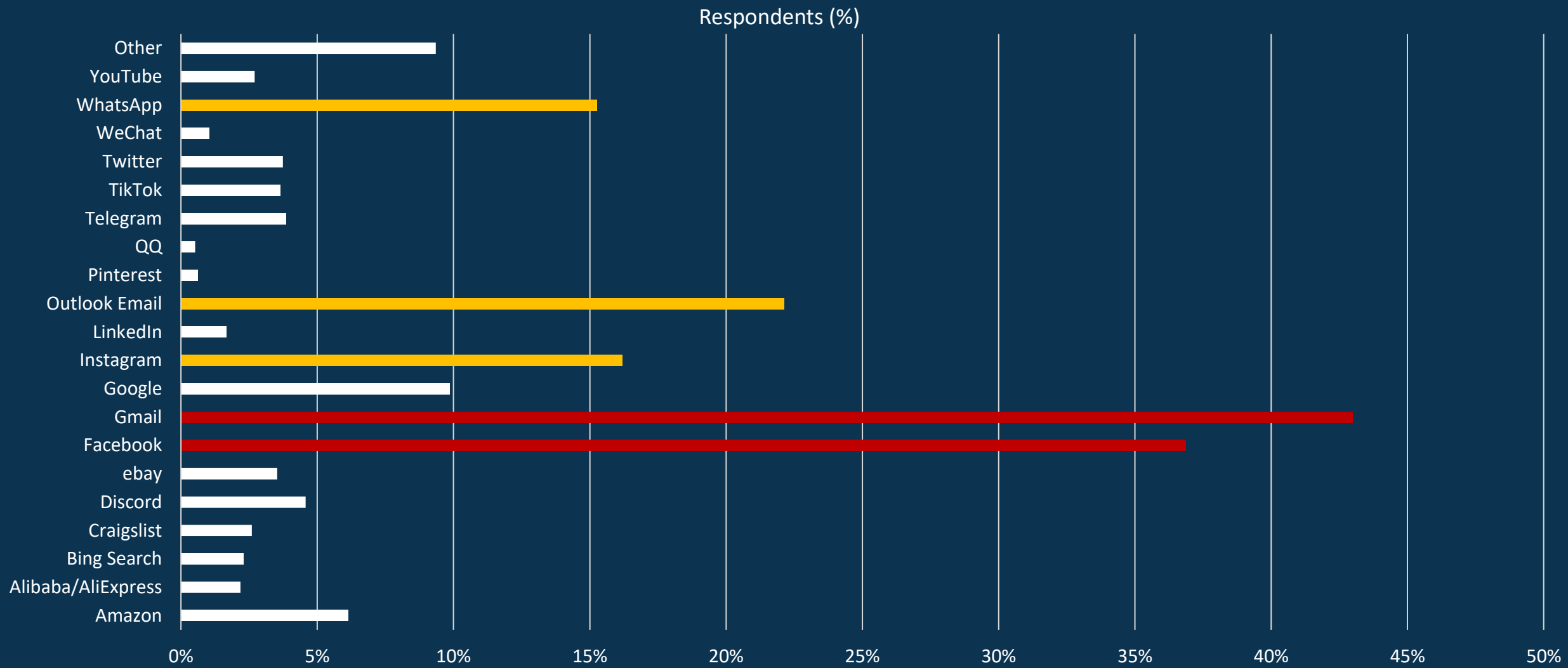
13% experienced fewer scams.

Most Kiwis receive scams via email



However, Text/SMS Messages, Phones, and Instant Messaging Apps are also common scam media.

Gmail and Facebook are the platforms most exploited by scammers

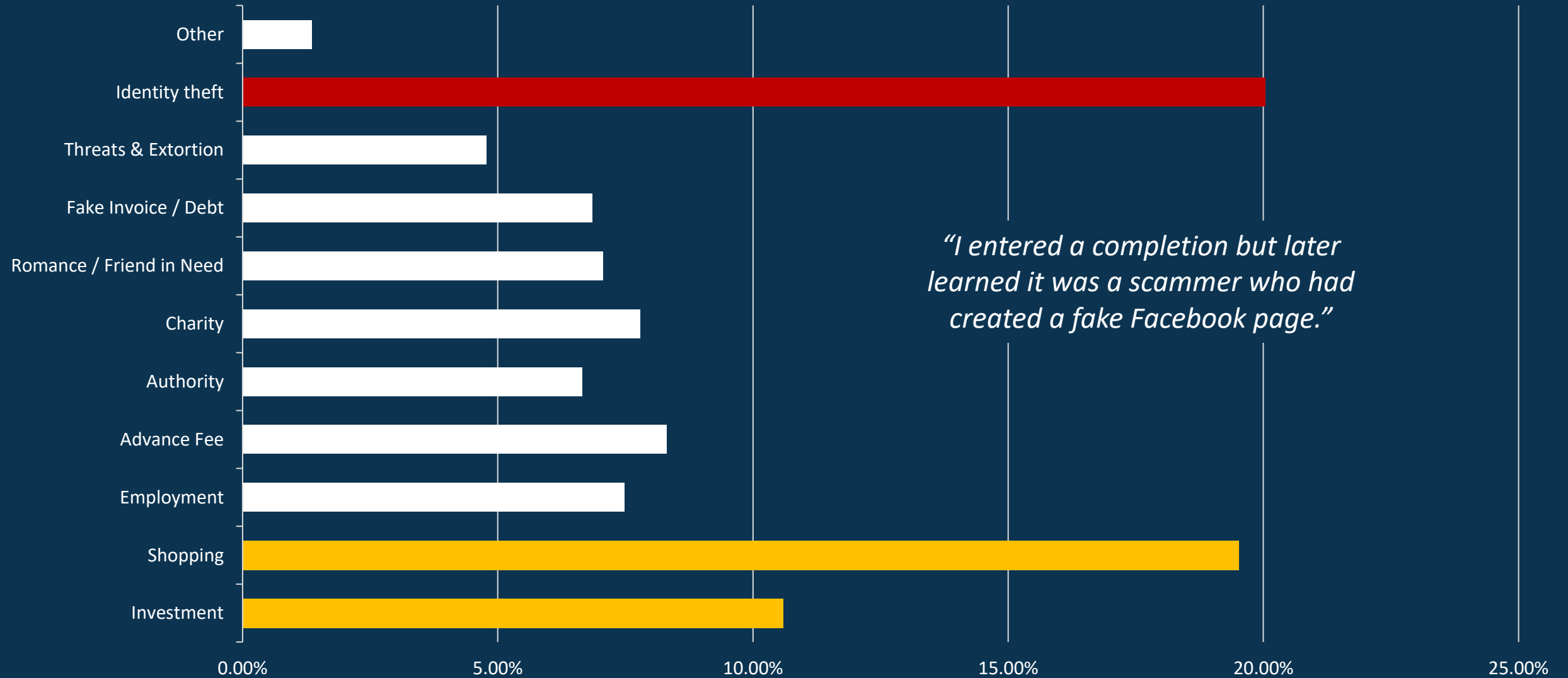


Outlook Email, Instagram, and WhatsApp take 3rd to 5th place.

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 scam in New Zealand

Respondents (%)

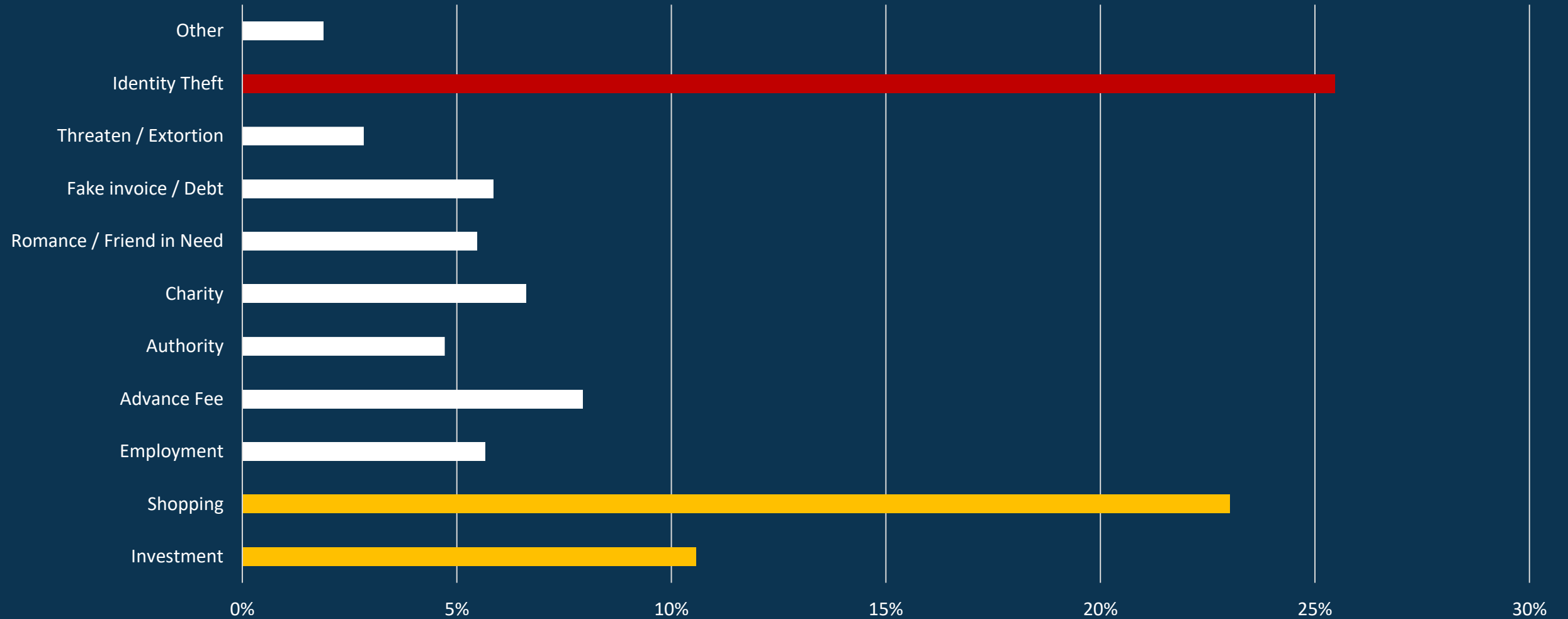


"I entered a completion but later learned it was a scammer who had created a fake Facebook page."

45% state none of the scams happened to them in the last 12 months. 1.8 scams were reported per scam victim.

Identity Theft & Shopping scams have the most impact on victims

Answers (%)



Followed by Investment scams.

Scams are hurting Kiwis in many ways

"Credit card information was used to make several unauthorised purchases. About \$400 was stolen from my account."

"I invested into a crypto mining site and it went well for a few weeks until they took the site offline."

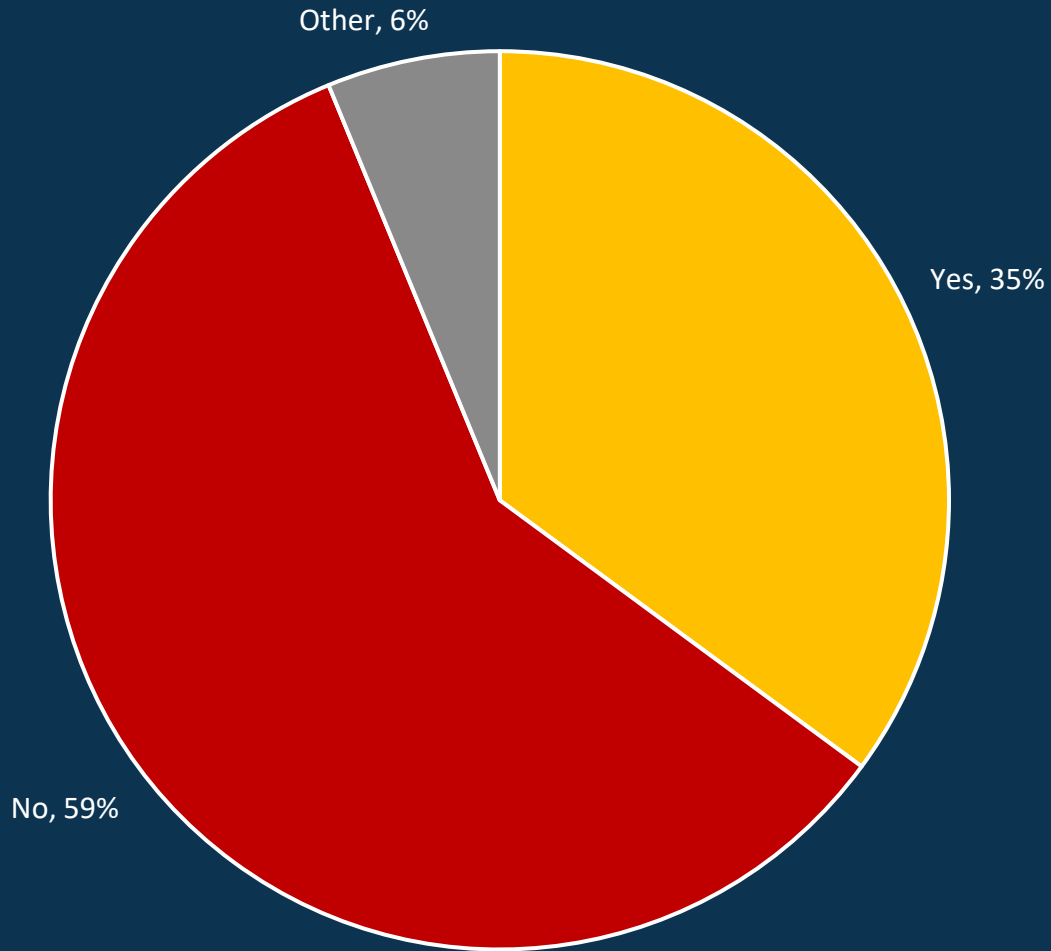
"I purchased some shoes off a website and never received them and when I tried to contact their customer service I got no reply."

"The 'cancer society' called to ask for donation and it turned out to be a fraud."

"I got advice that I would gain money from a charitable trust but had to pay a lawyer that they would supply to obtain this. It also stated that one of my Facebook friends had received the same grant. I tried to get hold of my friend with no success, so I googled the organisation and it was a reputable trust. I paid some money. They then tried to get more money so I then thought I had been conned & again tried to contact my friend & learned he had never heard of it."

59% did not report the scam to law enforcement

“Reported it to the bank and an official stockbroker.”

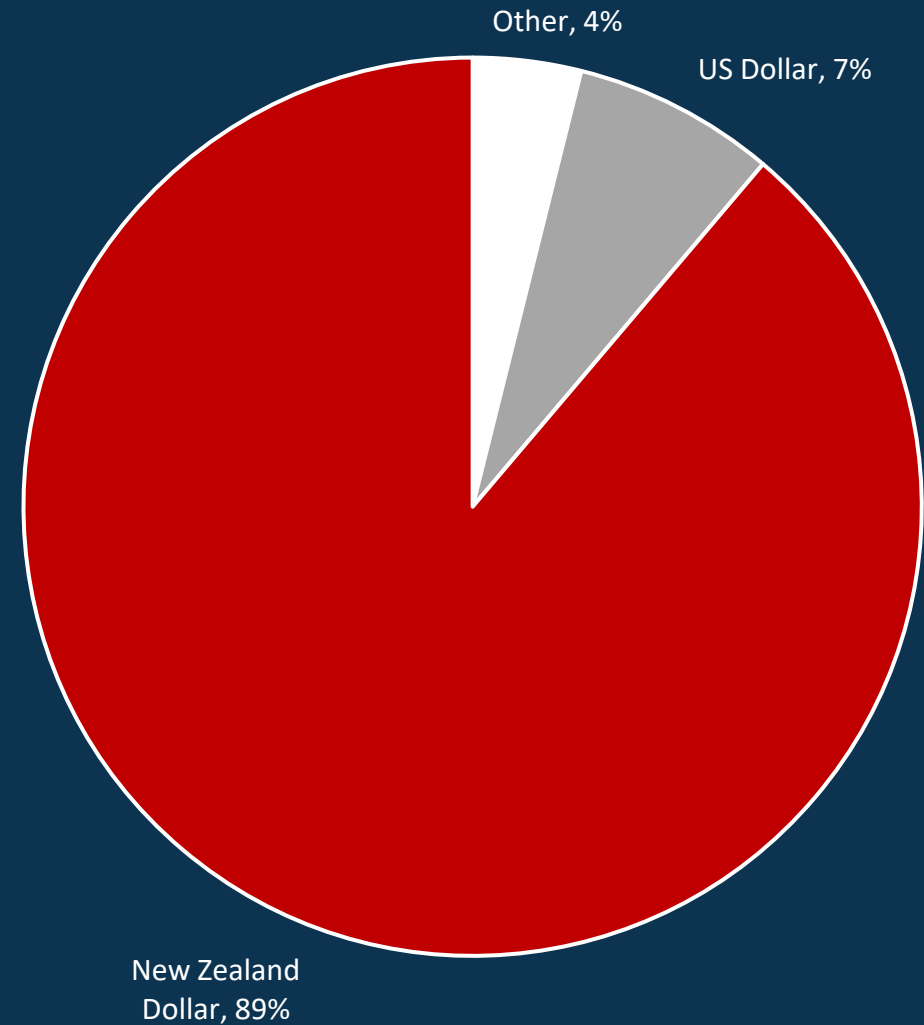


“I have notified my bank and they are looking into it.”

35% stated that they reported the scam to law enforcement or another government authority.

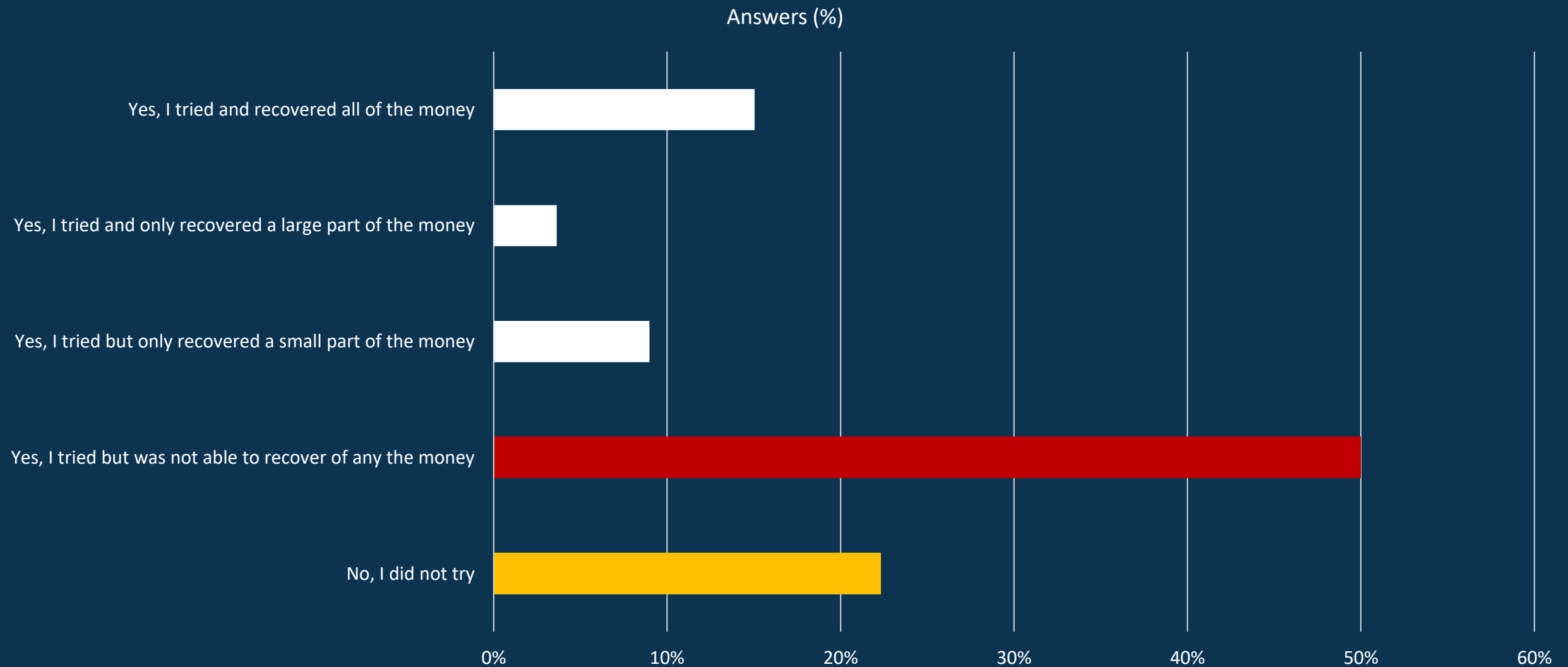
In total, 17% of the respondents who were approached lost money in a scam

Survey Key Statistics	
Number of persons approached	2,492
Participants completing the survey	50%
Participants losing money	412
% losing money / approached persons	17%
Average amount lost in US Dollars	\$ 1,846
Total country population	5,109,702
Population over 18 years	3,929,449
# of people scammed > 18 years	649,652
Total amount lost in scams*	US\$1,199,257,743
Gross Domestic Product (\$ millions)	251,969
% of GDP lost in scams	0.5%



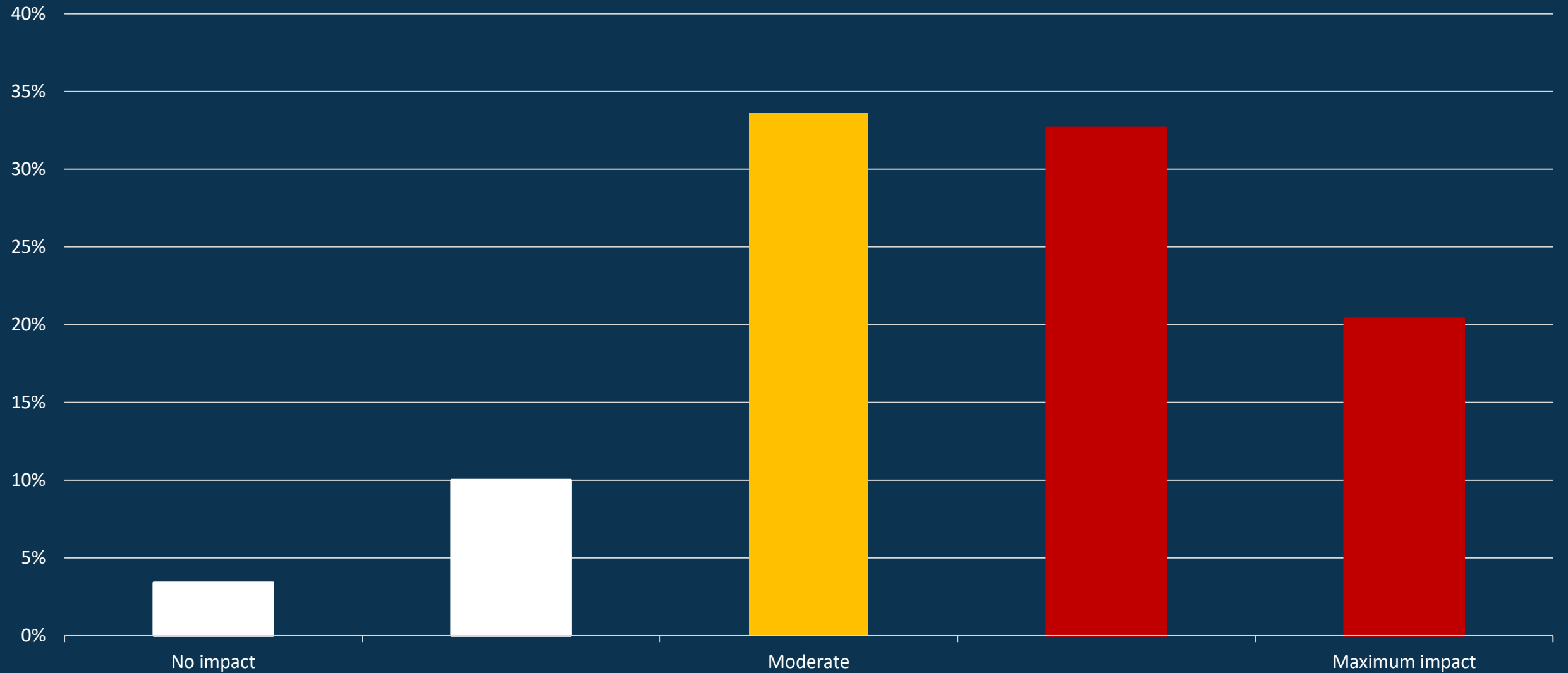
Most scams were reported in New Zealand Dollar and US Dollar.
Other currencies used were Bitcoin/ETH, UK Pound, Indian Rupees, Euro and South African Rand

Only 15% of the participants in the survey were able to recover all money lost



22% did not try to recover their funds. 50% tried but was not able to recover any money.

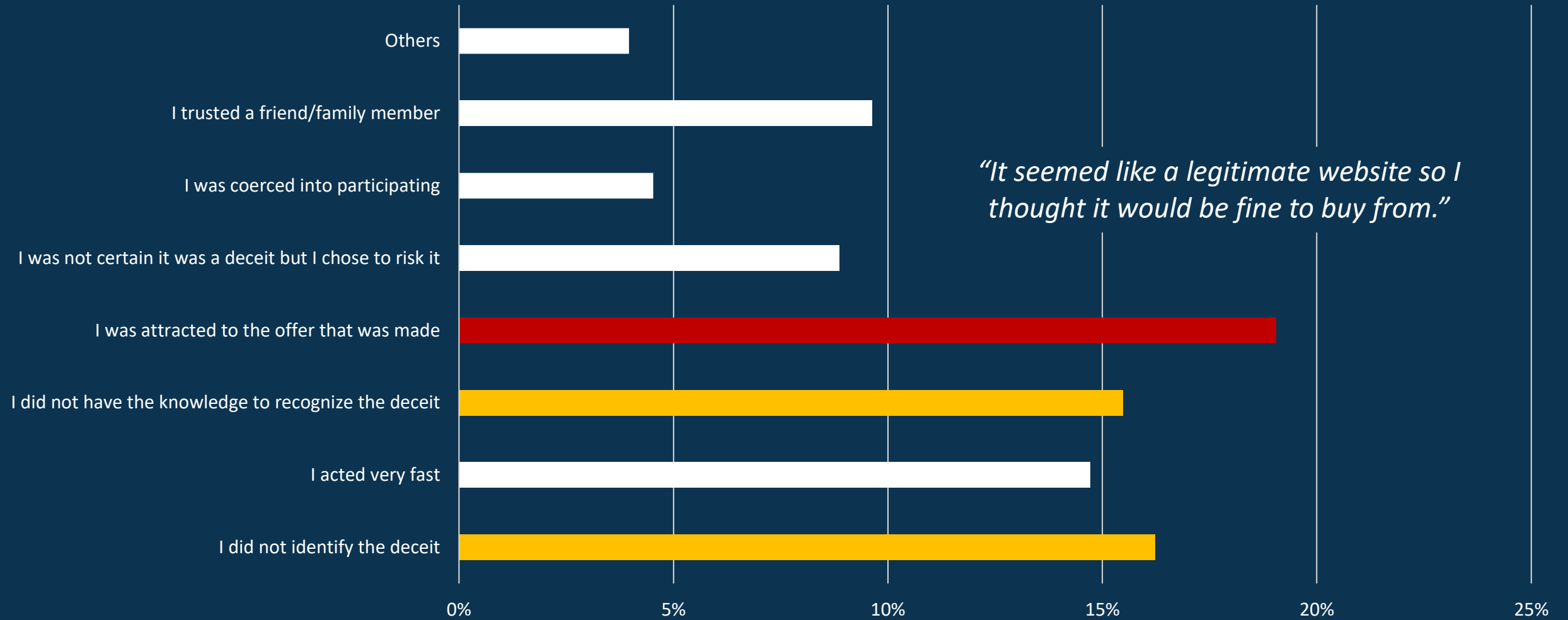
53% of the scam victims perceived a (very) strong emotional impact



13% of the participants reported no or little emotional impact.

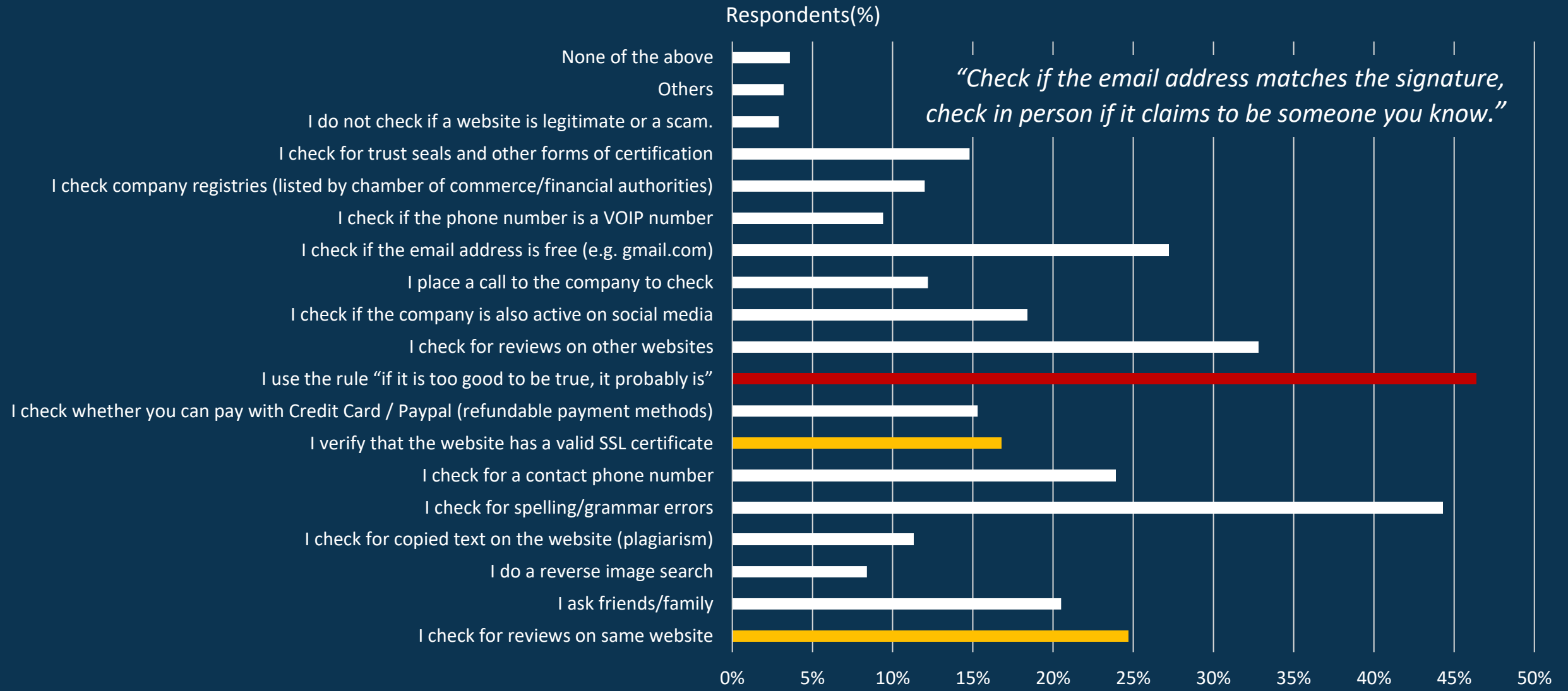
The main reason Kiwis fall for a scam is attraction to the offer made

Answers (%)



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

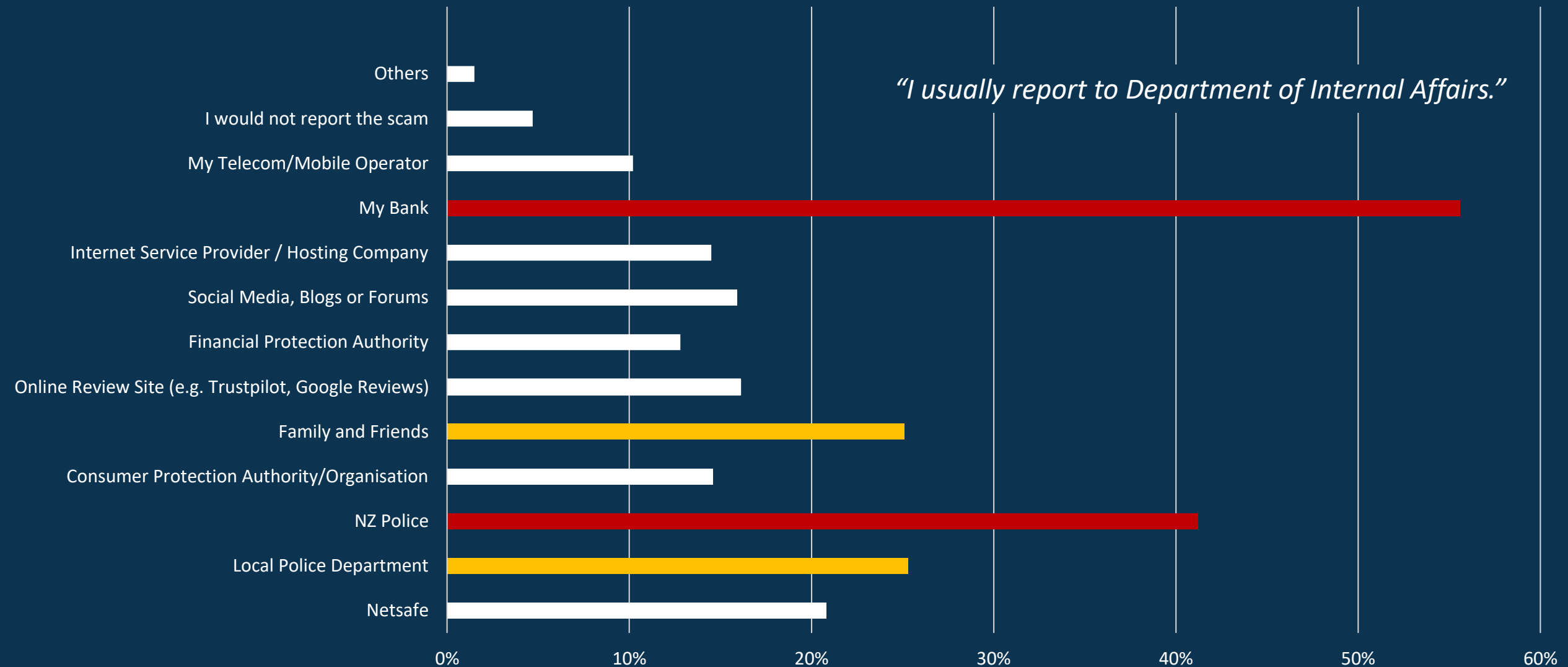
The most common scam check is “if it’s too good to be true, it probably is”



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

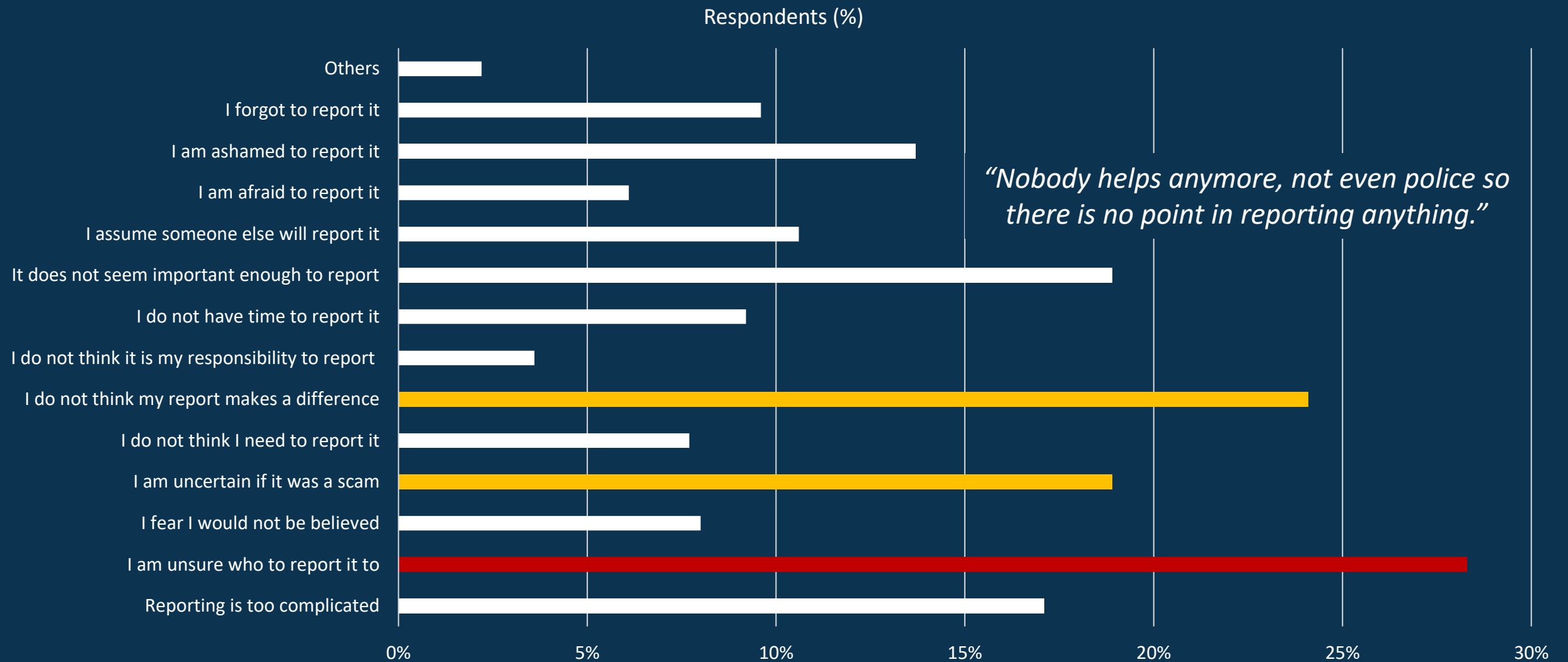
Scams are mostly shared with Banks and New Zealand Police

Respondents (%)



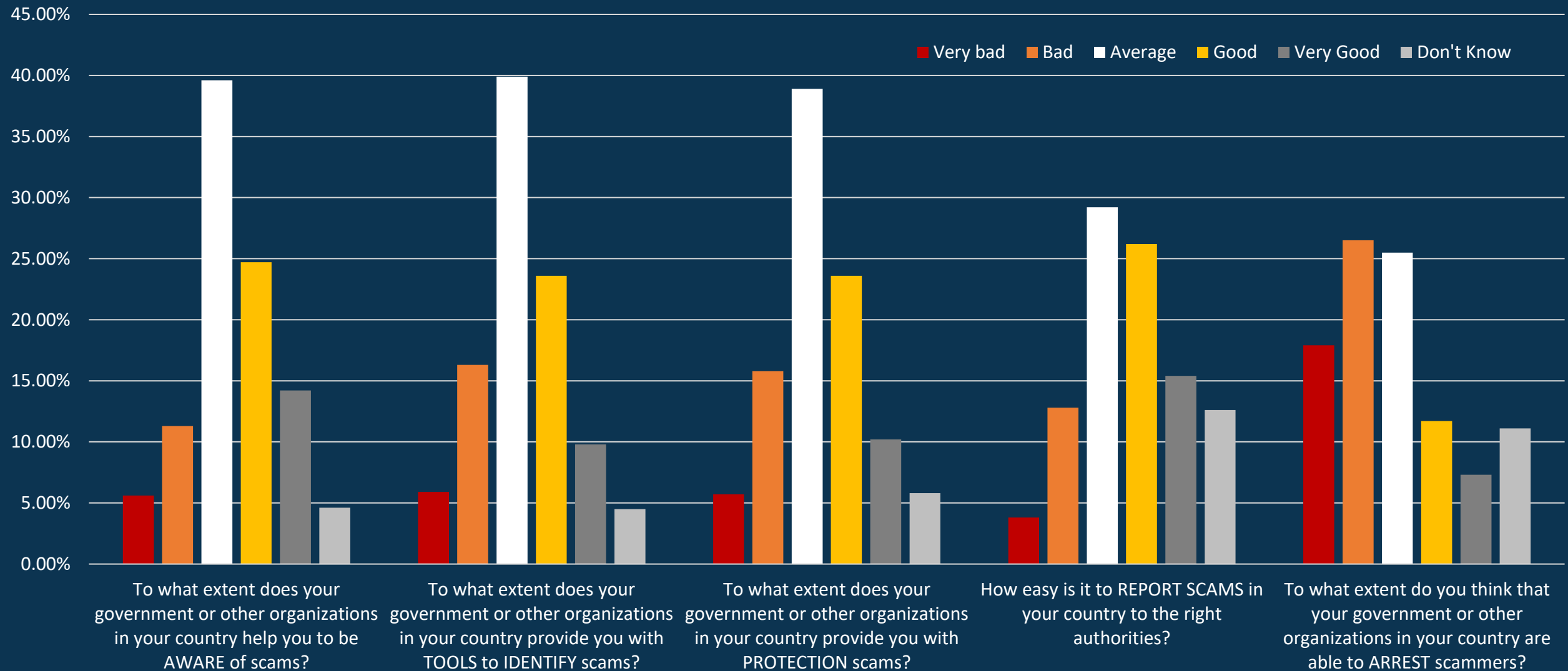
Local Police Department and Family & Friends are also popular scam report destinations.

The main reason for not reporting scams is uncertainty who to report to



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

Kiwis are displeased with the ability of the NZ authorities to arrest scammers



Overall, 24% of the participants rate the actions of the NZ government as (very) bad, 33% as (very) good.

Some remarkable quotes

“There needs to be a way that scammers can be prosecuted because right now if they are in another country nothing can be done. There should be a collective service (like UN) to help with this.”

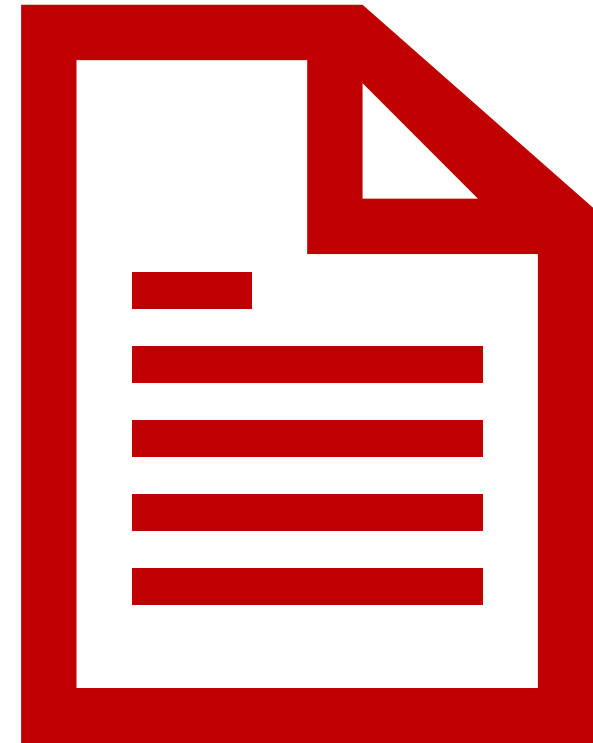
“We should protect our personal information and avoid disclosing it to untrustworthy sources!”

“The government should do more before more damage is done especially to the most vulnerable like the elderly. It should be made easy for scam reporting and the media should cover more of it to raise awareness.”

“If it seems too good to be true, it almost always is!”

“Most of the scam attempts I get are for undelivered postal items and requesting a fee for re-delivery, mostly from the NZ Postal Company. (I’ve) never heard of them.”

About this Report



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.

Netsafe is New Zealand's independent, non-profit online safety charity. Taking a technology-positive approach to the challenges digital technology presents, Netsafe works to help people in New Zealand take advantage of the opportunities available through technology by providing practical tools, support and advice for managing online challenges.



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 Hagenars 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 than 1. Hence bitcoin losses were not included in the estimate.

In addition to Pollfish we used the following sources:

- Inhabitants per country: [Worldometers.info](https://www.worldometers.info)
- Currency conversion: [Xe.com](https://www.xe.com)
- The country flag on the cover: [wikimedia.org](https://www.wikimedia.org)
- Internet penetration: [Wikipedia](https://www.wikipedia.org)
- GDP Estimate 2023: [Wikipedia](https://www.wikipedia.org)

The survey itself has been partly 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



Corporate Partners



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

Disclaimer

This report is a publication by the **Global Anti-Scam Alliance (GASA)** supported by **NetSafe**. 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

It is strictly prohibited to use information published in this report without the authors' prior consent. Any violation of such rule will result in a fine of €25,000, as well as in a further penalty of €2,500 for each day that such non-compliance continues. However, authors allows the use of small sections of information published in the report provided that proper citations are used (e.g., source: www.gasa.org)

Global Anti-Scam Alliance (GASA)

Oder 20 - UNIT A6311

2491 DC The Hague

The Netherlands

Email: partner@gasa.org

X (Twitter): @ScamAlliance

LinkedIn: [linkedin.com/company/global-anti-scam-alliance](https://www.linkedin.com/company/global-anti-scam-alliance)

