The State of Scams In Canada

feedzai

GASA
Global Anti-Scam Alliance

44% of Canadians targeted by scammers as C$13 billion is lost in 12 months

In the expansive landscape of Canada, a survey orchestrated by the Global Anti-Scam Alliance (GASA) and Feedzai painted a portrait of a nation increasingly ensnared in the web of deception spun by modern-day scammers. The data, built from the experiences of 989 Canadians, reveals not just numbers but stories of confrontation, loss, and the ongoing struggle against scams.

The survey participants, more women than men, spanned across all ages, a testament to the indiscriminate nature of scams. These individuals, many armed with vocational education, formed a tapestry of experiences and backgrounds. The majority stood confident, with 68% believing in their ability to recognize the fraudulent calls and messages that have become all too common. Yet, there were those, 7% to be precise, who confessed their vulnerability, not quite sure of their ability to discern the honest from the dishonest.

As the seasons turned, so too did the frequency of scam encounters. A striking 75% of Canadians reported coming across a scam at least once a month, while 14% noticed them every few months. In a concerning trend, over half of the respondents noticed an increase in scam attempts over the past year, and only a minor 9% saw a decrease.

The channels through which these scams slithered into lives were primarily phone calls and emails, with Gmail and Facebook being the most exploited platforms. Scammers also weaved their deceit through Outlook, WhatsApp, and Instagram, creating a network of online traps.

The cost of these scams was not trivial. Of the surveyed, 44% had been successfully targeted, leading to an average financial loss of C$2,406 (US$1,762) per person. The collective loss amounts to an estimated C$13 billion (US$9.5 billion), or 0.5% of Canada's GDP. Most of these transactions were in Canadian dollars, although US dollars were also commonly scammed.

Despite the high encounter rate, a majority of 69% chose not to report these scams to law enforcement. This decision was multifaceted, with some not knowing where to report, others deterred by complicated processes, and a few fearing the repercussions of reporting.

For the 27% who did report, their actions reflected a glimmer of agency in the grim narrative. Still, the emotional toll was undeniable, with 47% of scam victims reporting a strong emotional impact, illustrating that the scars left by scams are not solely monetary.

The narrative of why Canadians fall victim to scams is woven with threads of allure and urgency. Offers too tempting to ignore, and decisions made in haste, were common culprits. Common wisdom such as "if it seems too good to be true, it probably is," served as the primary checkpoint for many, but not all defenses held strong. Some relied on less reliable methods like checking reviews on the same site where the scam appeared or trusting in the presence of SSL certificates.

In the aftermath, those affected often turned to their banks and local police departments for aid, though many shared their experiences with family, friends, and online review sites. Yet, the landscape of reporting was marred by confusion and disillusionment, with many feeling disheartened by the government's response to their plights. More than half expressed dissatisfaction with the government's efforts to combat scams, and many longed for a more vigilant and punitive approach.

The survey's findings lay bare a complex and troubling issue that touches Canadians from all walks of life. The responses narrate a collective experience marked by challenges and the search for resilience in the face of a digital epidemic. Through numbers and personal accounts, the survey chronicles a nation's encounter with scams and the urgent need for a more robust defense against this growing threat.

Jorij Abraham

Jorij Abraham, Managing Director, Global Anti-Scam Alliance

44% of Canadians targeted by scammers as C$13 billion is lost 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 3 out of 4 Canadians experience a scam on a monthly basis. Unfortunately, 69% of Canadians don't report scams to law enforcement – which is 7% higher compared to Americans. Canadians don't report because 1) they don't know where to report it, or 2) they don't think it would make a difference. Interestingly, about 55% of Canadians turn to their banks when they fall victim to scams – 5% higher than Americans – and may indicate that Canadians instill more trust in their bank. This gives financial institutions 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.

The introduction of the Real-Time Rail in Canada will bring convenience to consumers, financial institutions, payment service providers, and government agencies. But this also poses plentiful opportunities for scammers to get money from victims even faster – leaving either the consumer or the financial institution to take the loss. This means Canadian banks and payment service providers must identify and stop fraud before the point of transaction. Taking a proactive, preventative approach minimizes the fraud losses associated with real-time and instant payments.

We need a collaborative approach to stand a chance in the fight against scams. This means banks, big tech companies, 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.

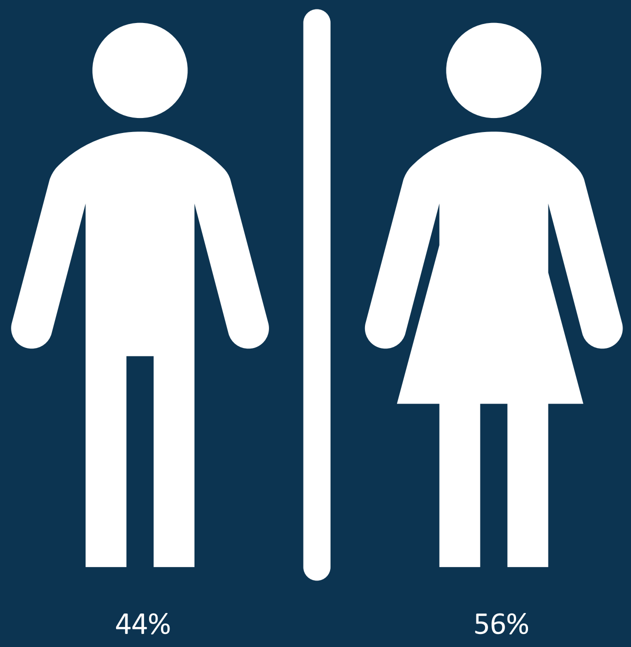
3. **Consumer education**: Financial institutions can deploy a variety of scam education tactics. At minimum, banks can display warning messages before the consumer can complete the transaction. But other banks have email campaigns to inform consumers about the latest scam trends, its scale, and how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

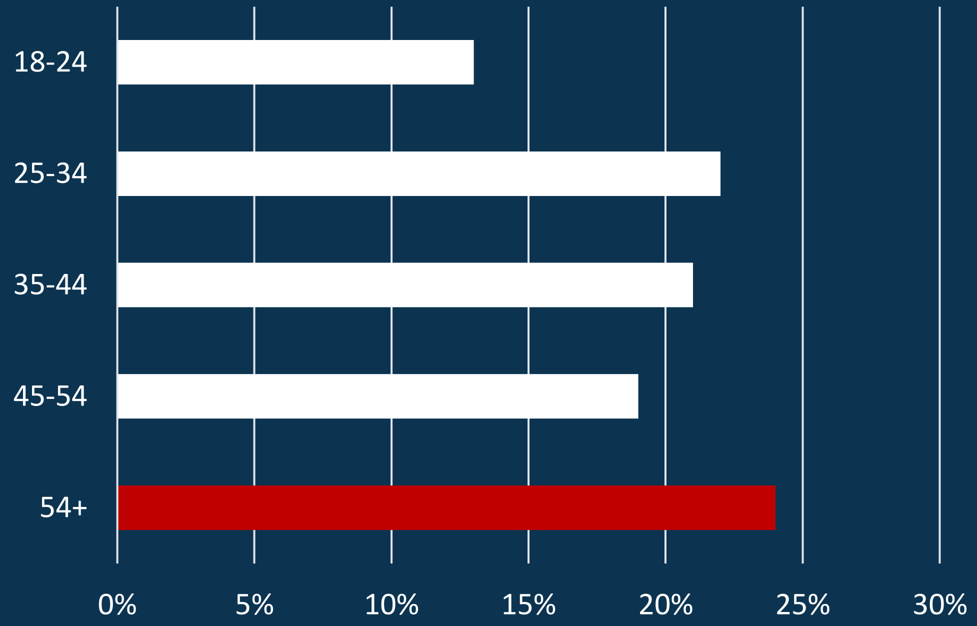
Feedzai is a proud partner of GASA and aims to equip financial institutions with the tools they need to prevent scams and protect consumers. Learn more about Feedzai here.

Brett Barrett, Vice President, Feedzai

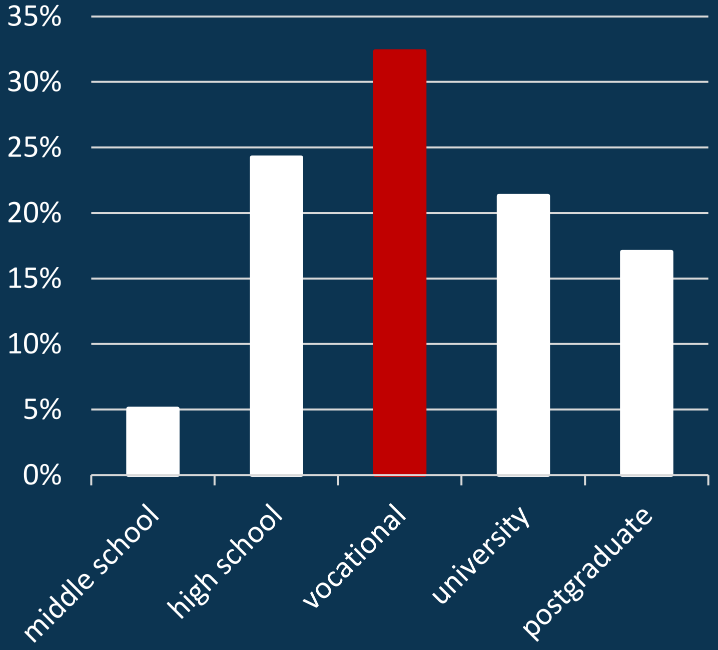
989 Canadians participated in the survey



Gender



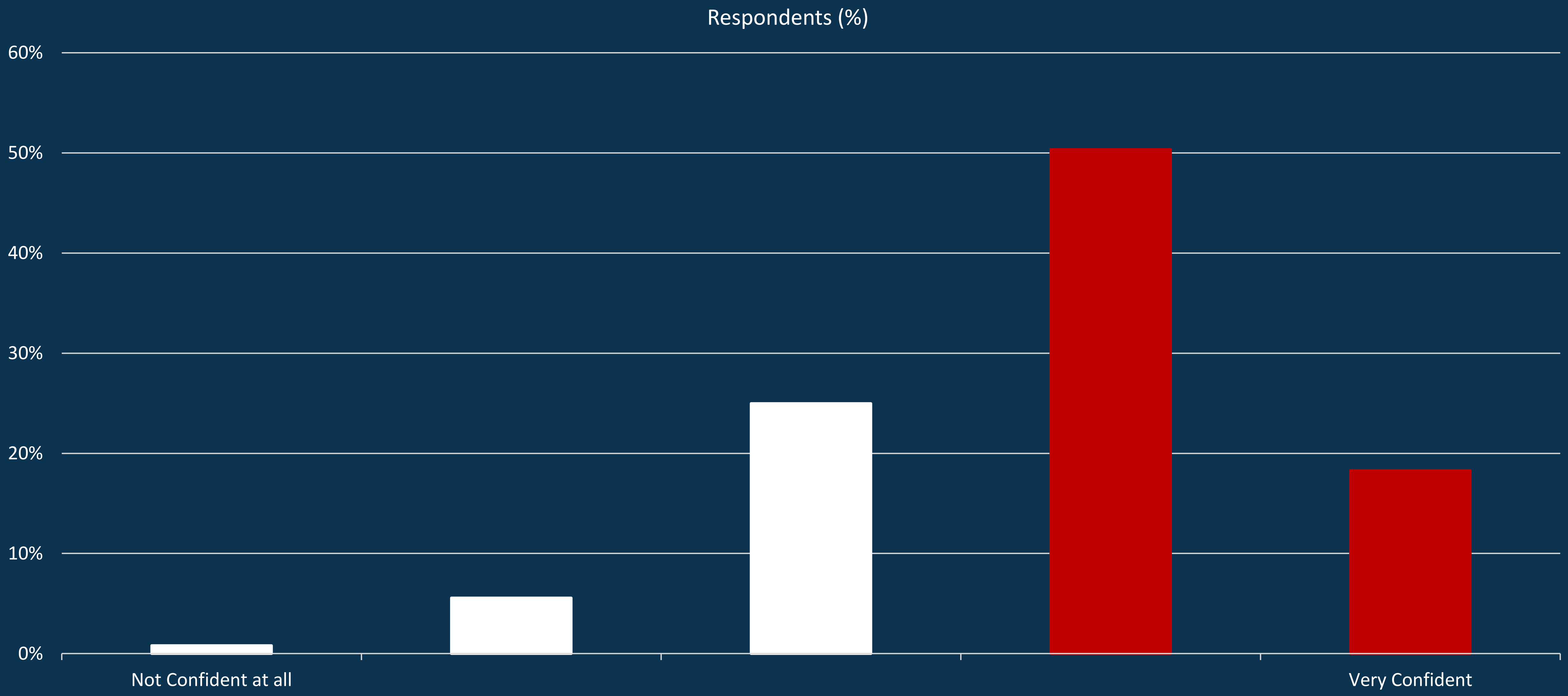
Age



Education

More women participated than men, in a relatively even representation across age groups, with a vocational education.

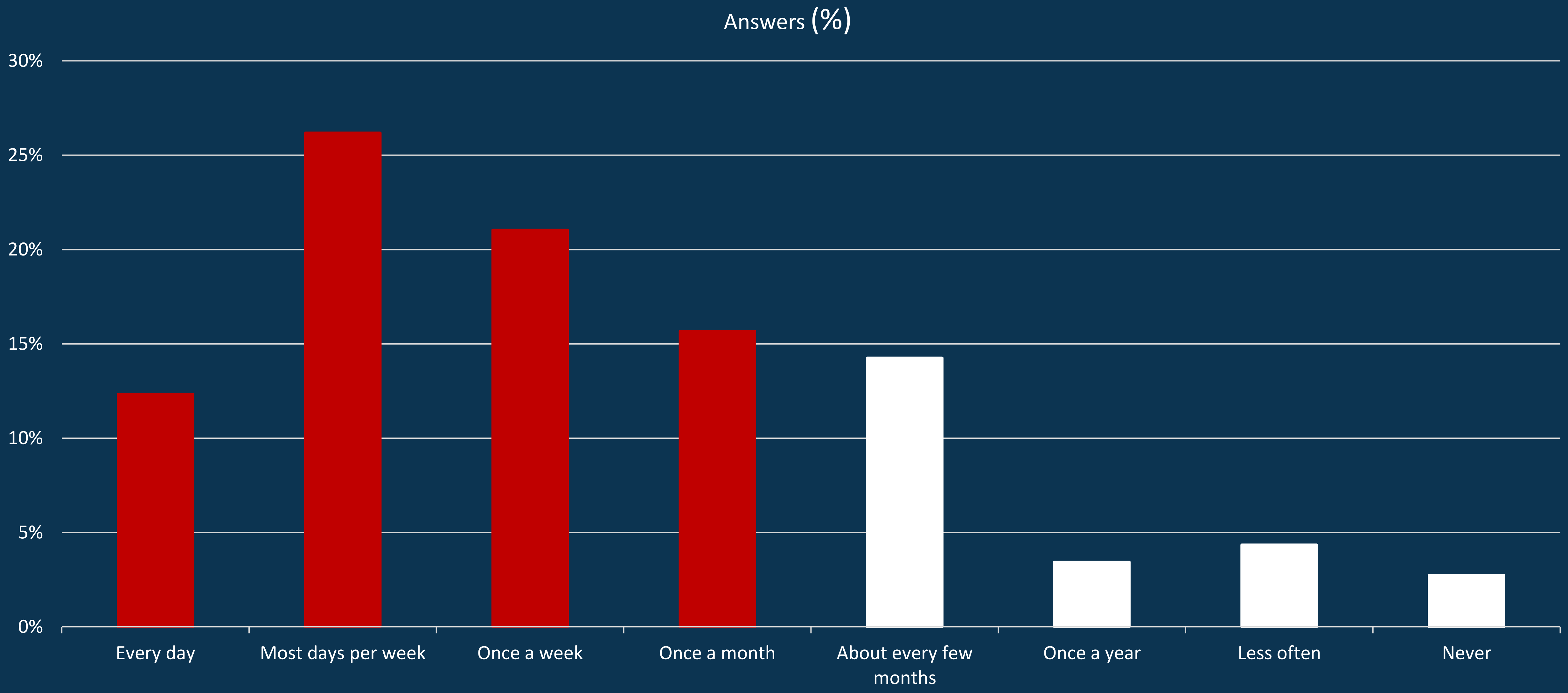
68% of the Canadians are (very) confident that they can recognize scams



Only 7% is not (very) confident at all.

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

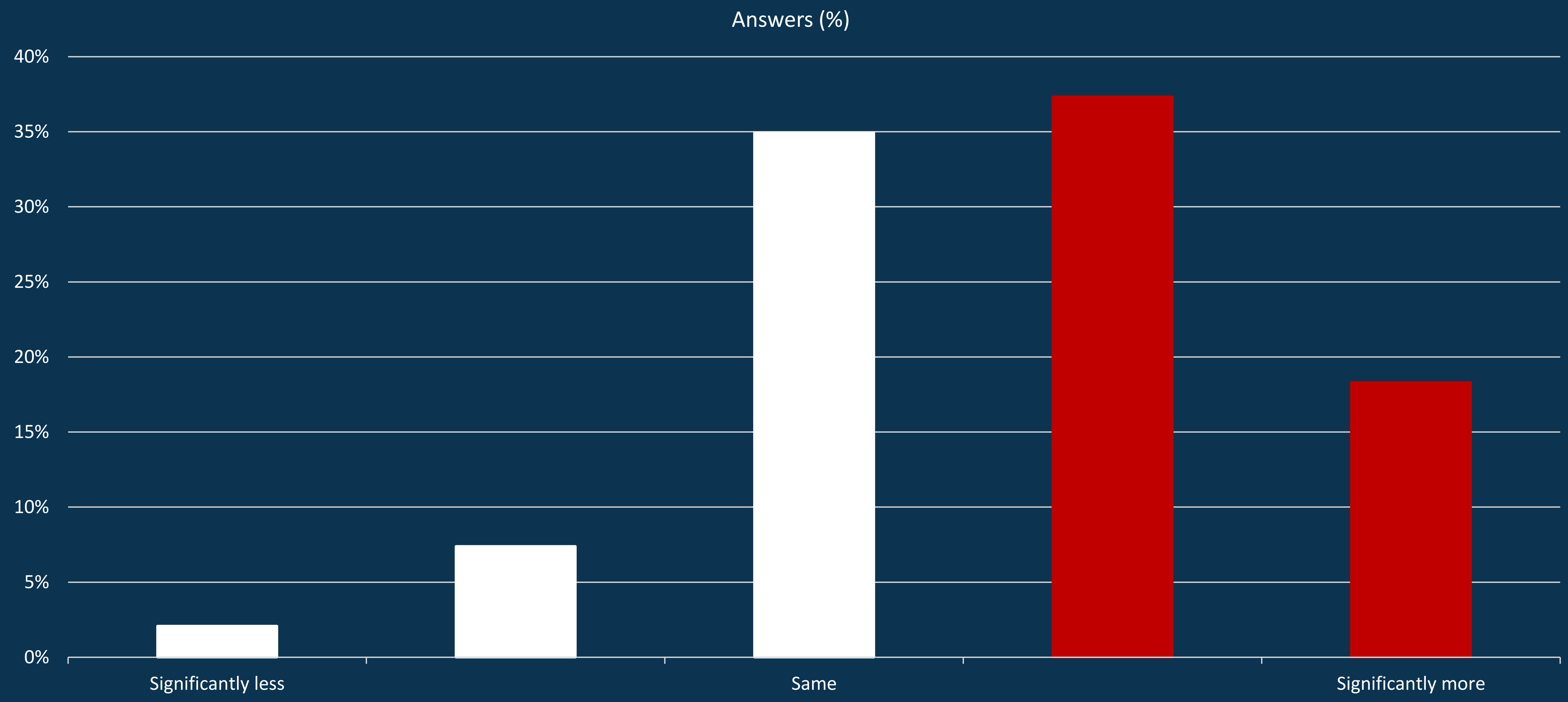
75% of the Canadians encounter a scam at least once per month



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)?

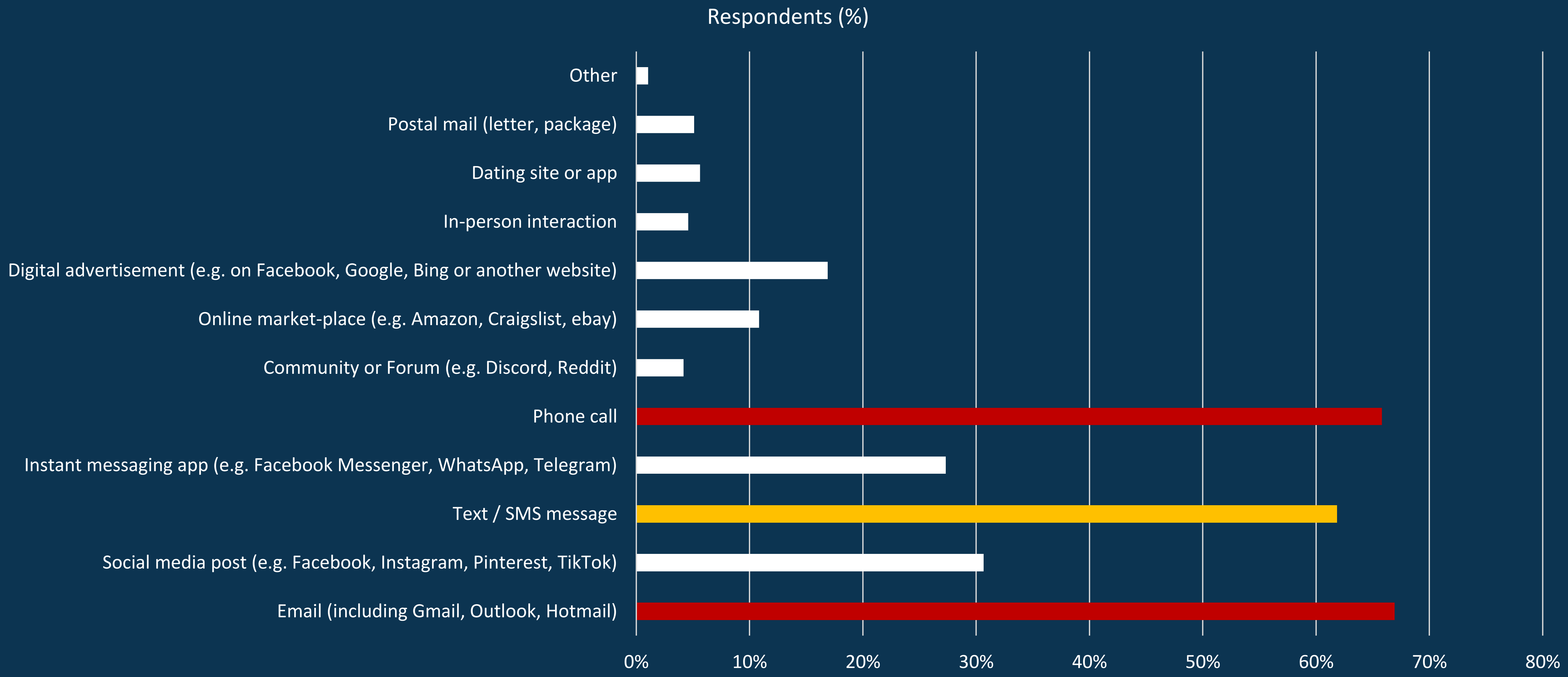
56% of the Canadians experienced more scams in the last 12 months



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?

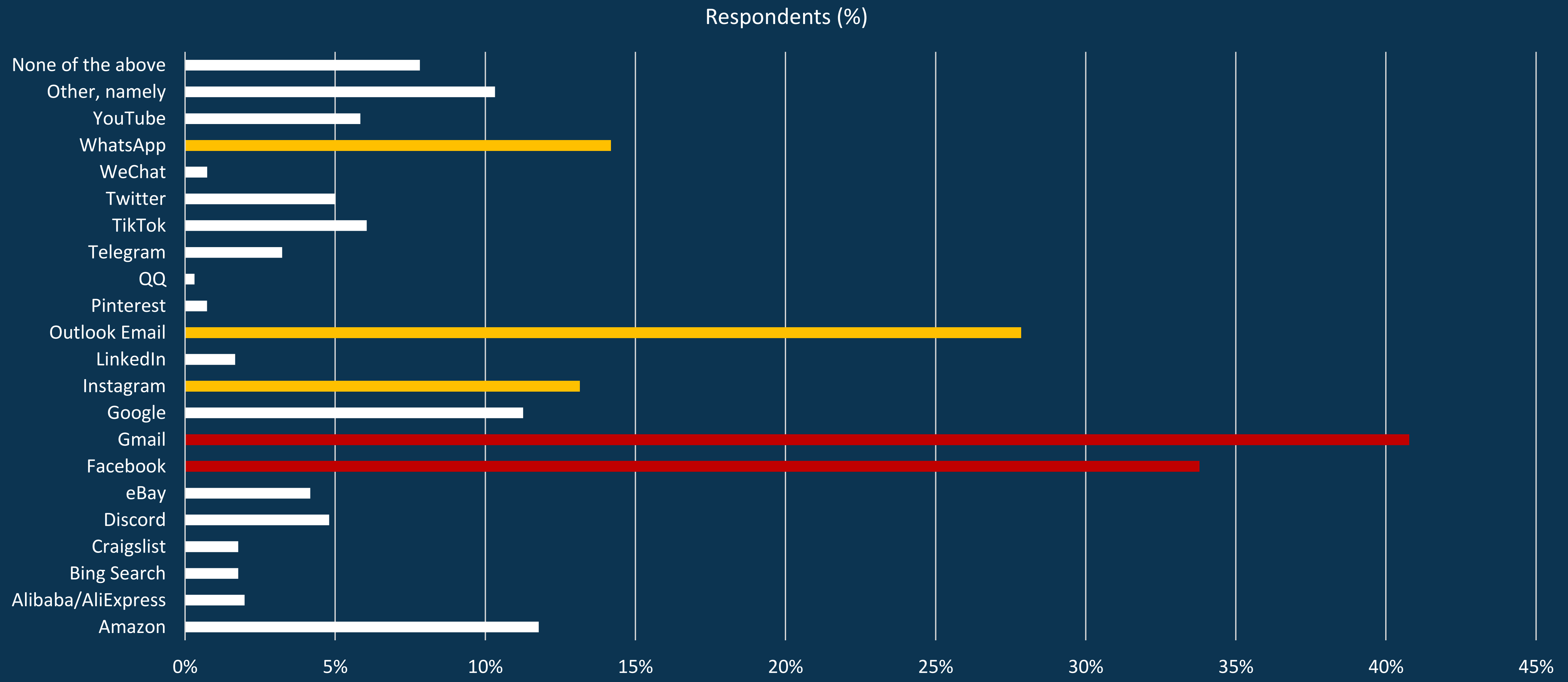
Most Canadians receive scams via Phone calls and Emails



However, Text/SMS messages and social media 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.

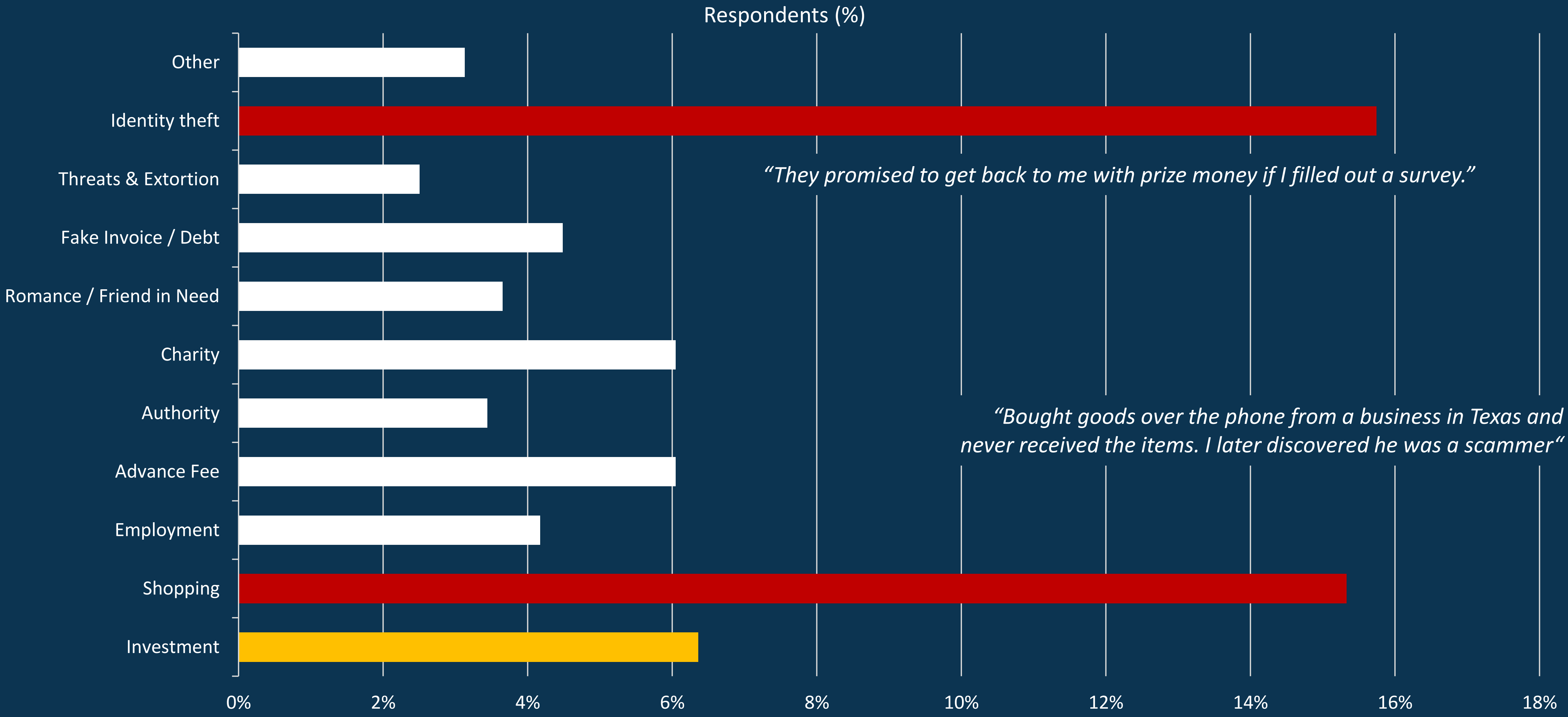
Gmail and Facebook are the most used platforms by scammers



Outlook Email, WhatsApp, 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.

44% of the Participants reported being scammed



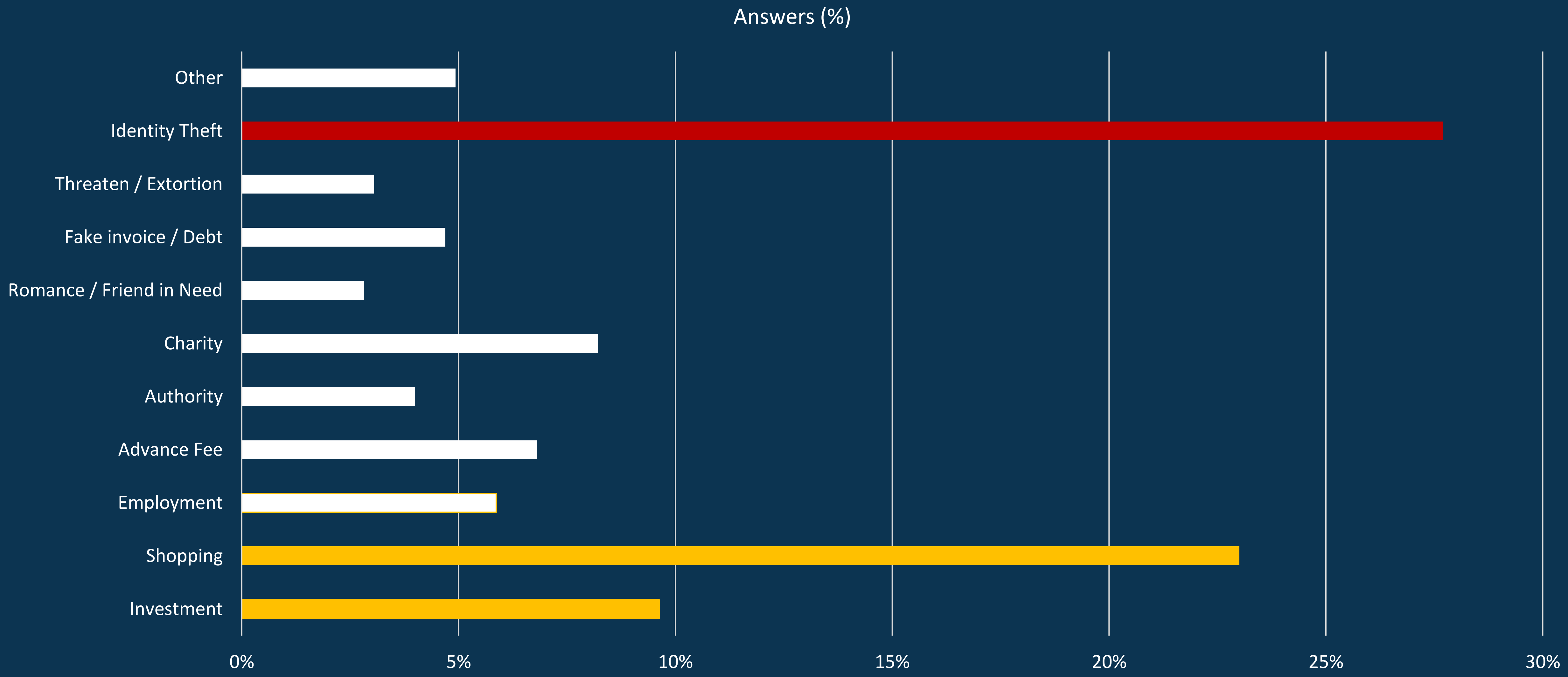
“They promised to get back to me with prize money if I filled out a survey.”

“Bought goods over the phone from a business in Texas and never received the items. I later discovered he was a scammer“

Identity Theft and Shopping Scams are the most common scams in Canada, followed by Investment schemes
Scam Victims were scammed 1,59 times in the last 12 months

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 Shopping and Investment Scams.

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

Scams are hurting Canadians in many ways

“I was told by a friend to invest some money and I'll get double profit. I did and I got paid then I tried again then I go scammed.”

“Paid for a kitchen aid mixer that I have never received. Contacted the seller, was told the product has reached my country there’s nothing they can do…”

“They called me and convinced me to donate money to sick kids' hospital, turned out to be fake and scam.”

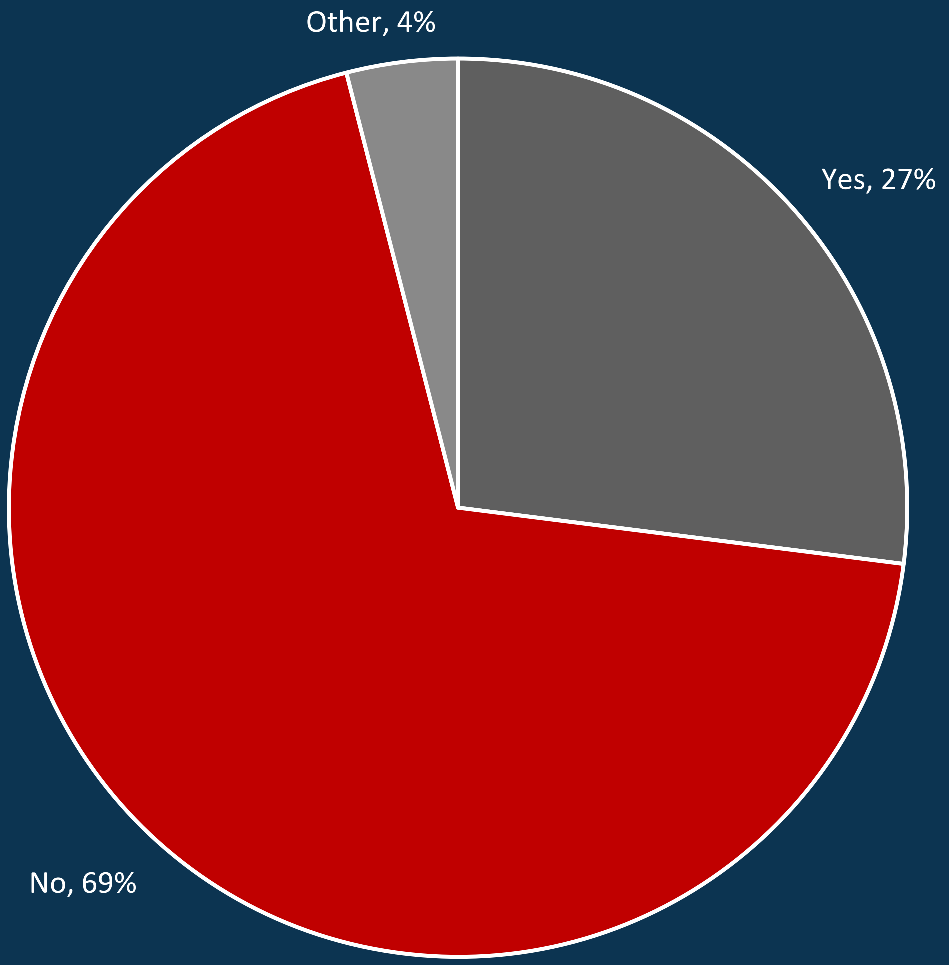
“I was told that I received a $750 gift card on Instagram but they requested $2 to mail it to me.”

“My credit card was compromised and there was a transaction every day for 2 weeks.”

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

69% did not report the scam to law enforcement

"I reported to Mastercard."



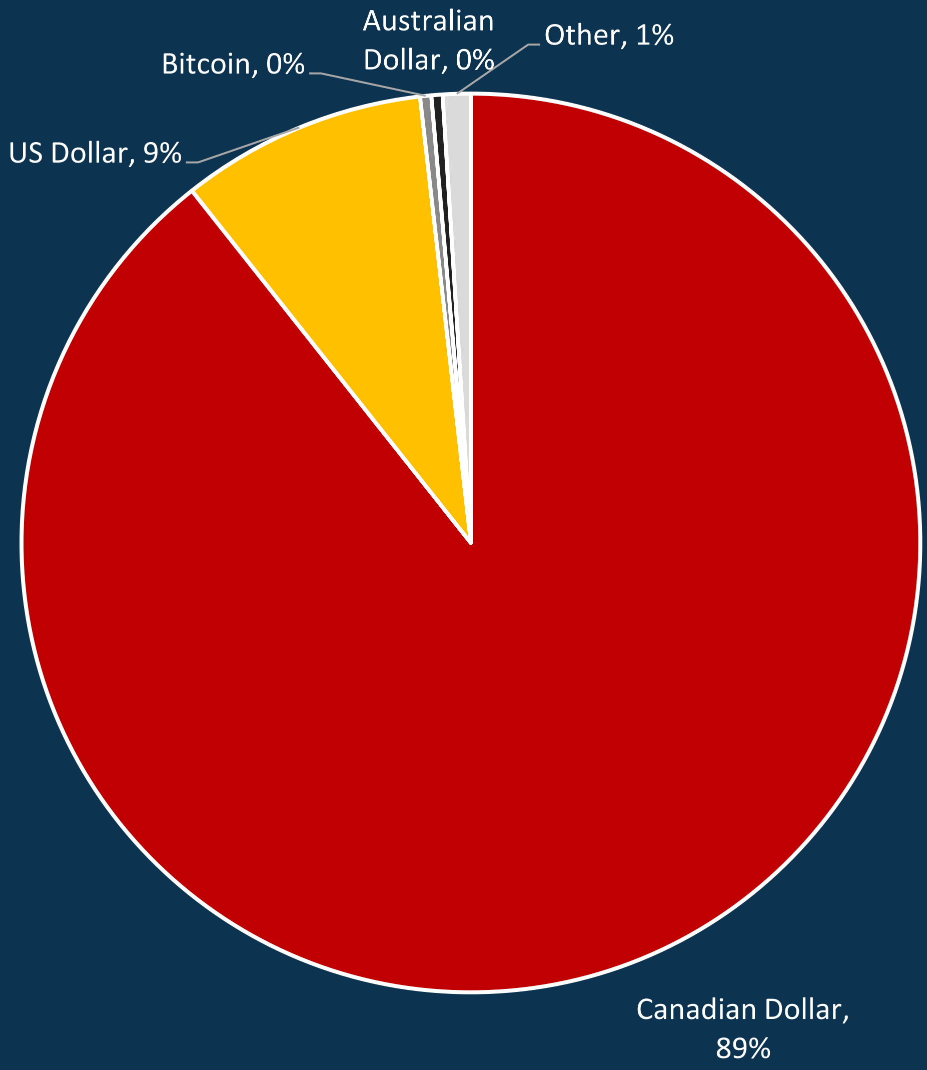
"I reported it to the bank and they investigated. I don't know the conclusion of the investigation"

27% stated that they 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 those surveyed reported losing money in a scam

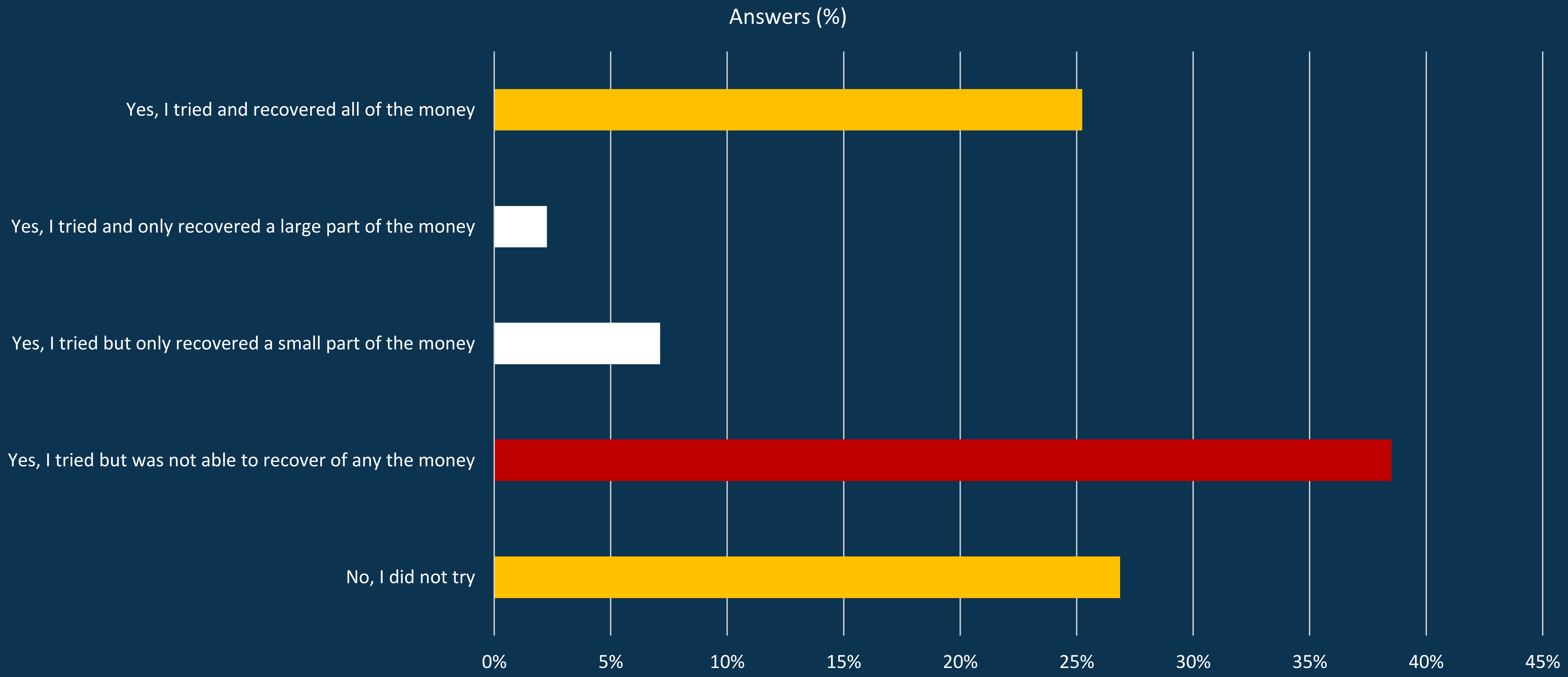
Survey Key Statistics	
Number of persons approached	1,789
Participants completing the survey	55%
Participants losing money	309
% losing money / approached persons	17%
Average amount lost in US Dollars	US$ 1,762
Total country population	38,516,736
Population over 18 years	31,236,789
# of people scammed > 18 years	5,395,287
Total amount lost in scams*	US$ 9,506,495,062
Gross Domestic Product ($ millions)	2,089,672
% of GDP lost in scams	0.5%



Most scams are in Canadian Dollars (89%), the remainder is mainly in US Dollars (9%).

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".

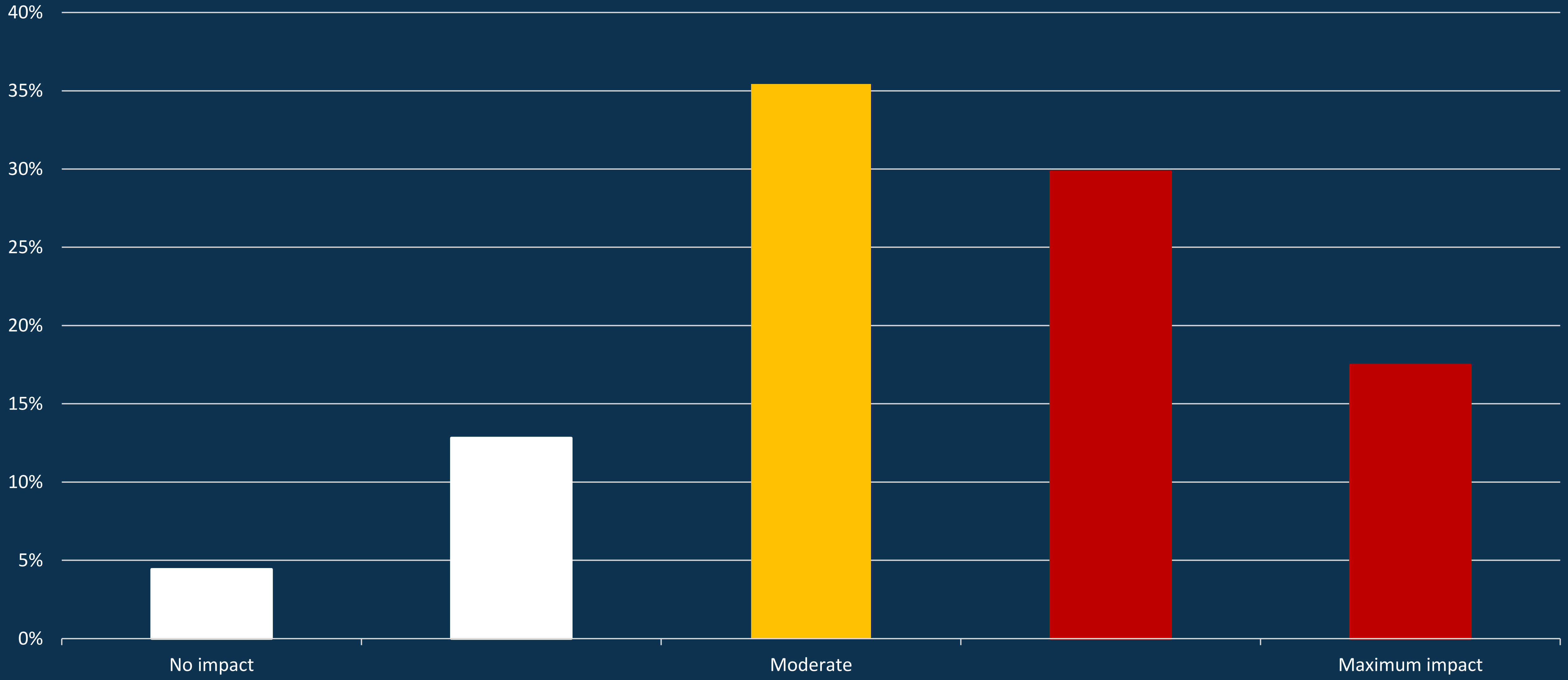
25% of the participants in the survey were able to recover all money lost



27% did not try to recover their funds. 39% tried but was not able to recover any money.

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

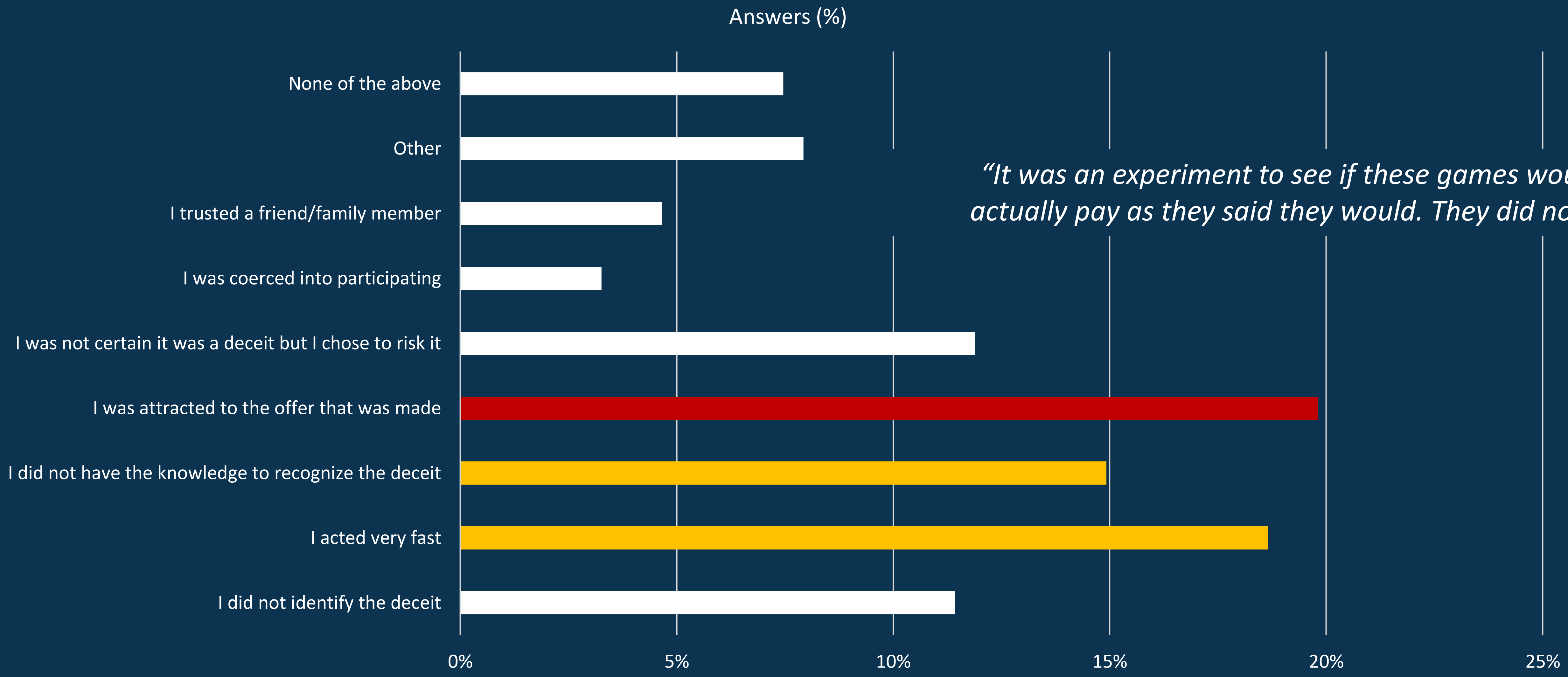
47% of the scam victims perceived a (very) strong emotional impact



17% 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 reasons Canadians fall for a scam is the attraction of the offer

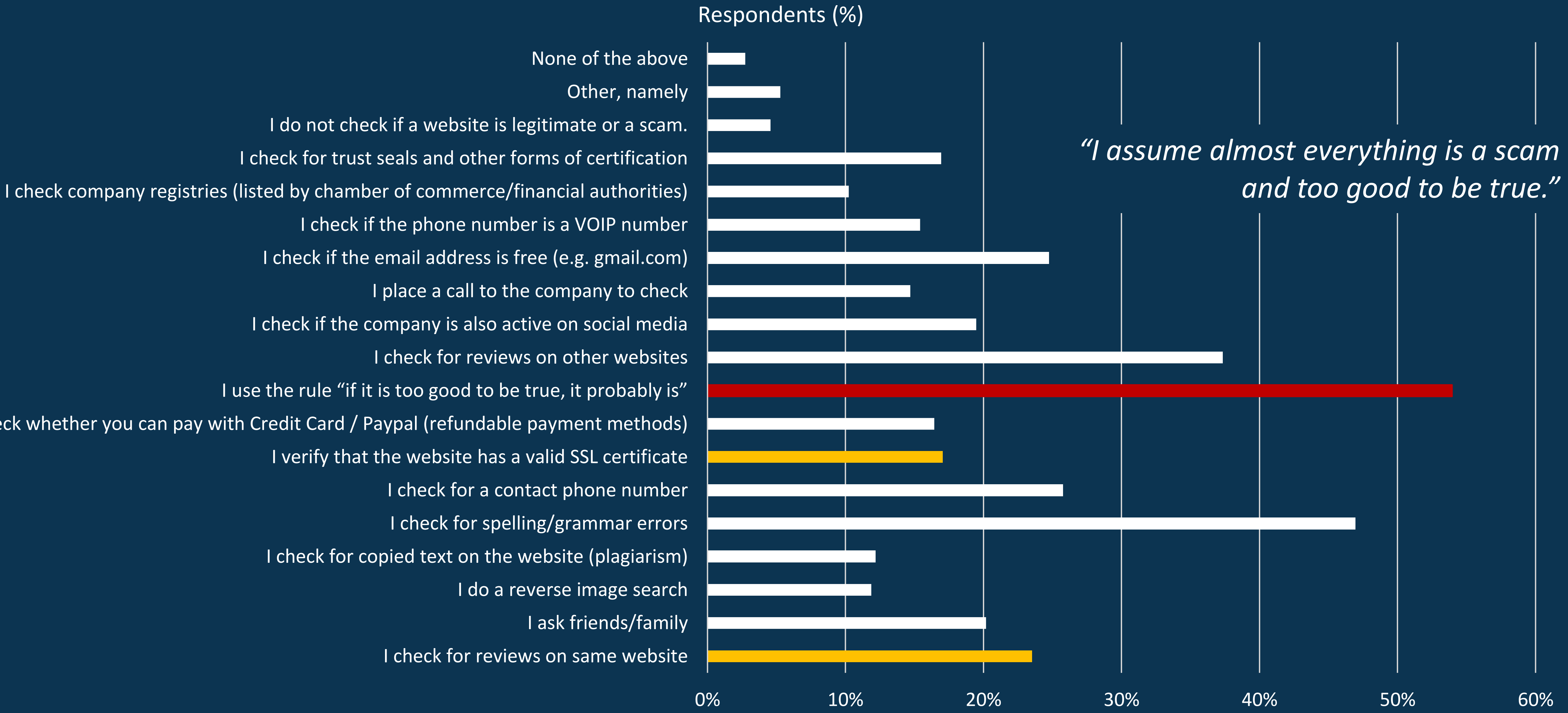


“It was an experiment to see if these games would actually pay as they said they would. They did not.”

Several victims also reported they did not have the knowledge to recognize the deceit or acted very fast.

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”

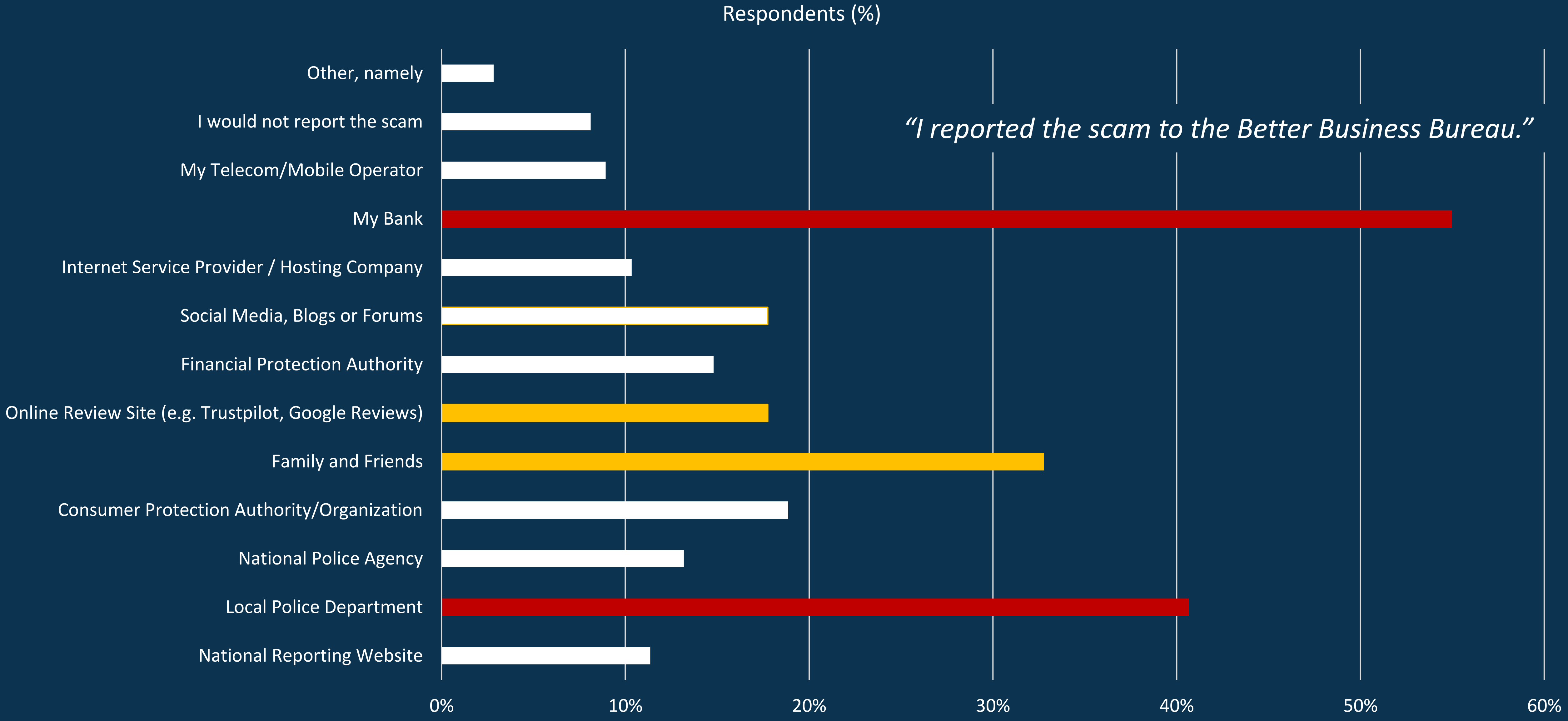


“I assume almost everything is a scam and too good to be true.”

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

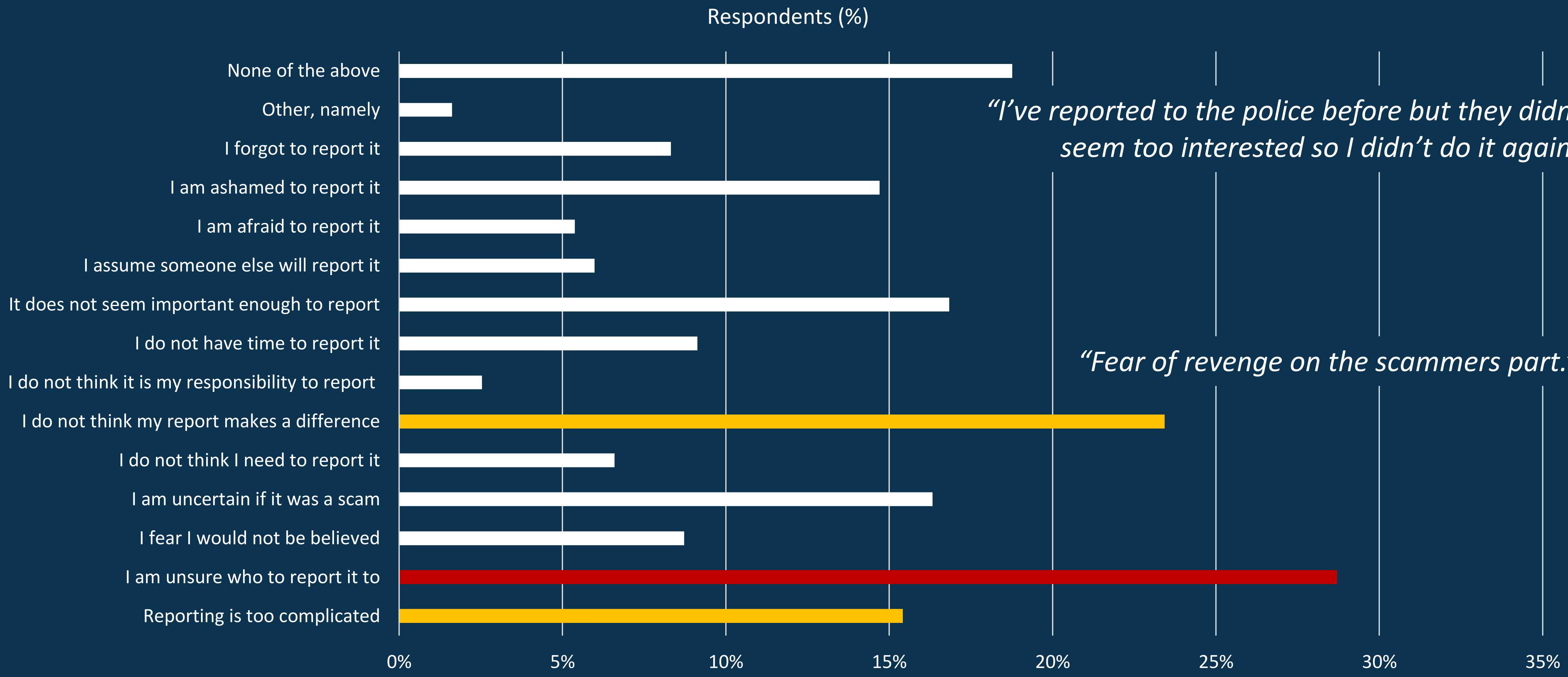


"I reported the scam to the Better Business Bureau."

Family & Friends and Online Review Sites are also popular scam reporting methods.

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

Not being sure where to report is the main reason for not reporting scams



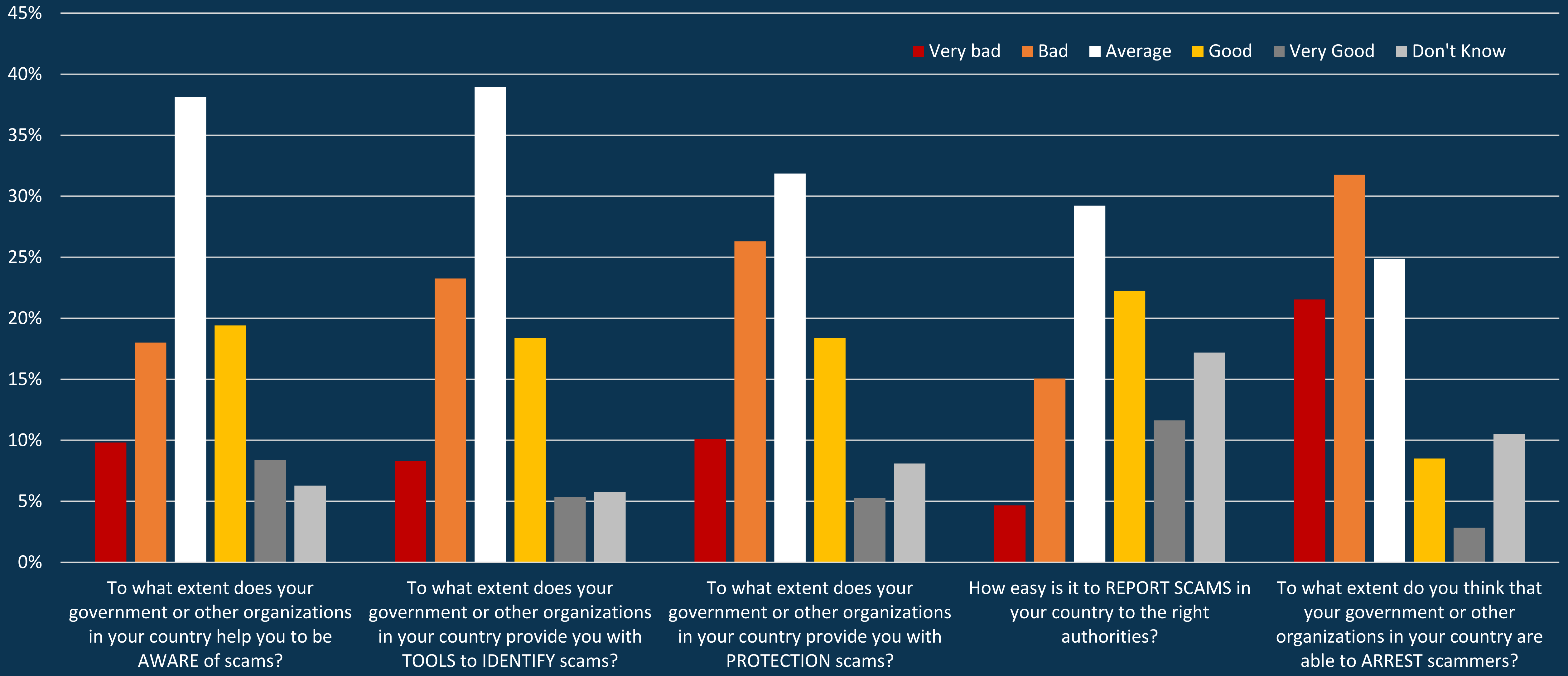
"I've reported to the police before but they didn't seem too interested so I didn't do it again."

"Fear of revenge on the scammers part."

Other key reasons for are the reporting process being too complicated and uncertainty that reporting will make a difference.

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

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



Overall, 34% of the participants rate the actions of governments as (very) bad, 24% 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

“I wish they would be severely punished They are getting very creative with their scams.“

“Need to be more vigilant about the scammers.”

“I think scams become worse nowadays. I’m very anxious. I’m afraid sometimes to use my phone on the computer. People who scam are able to enter in your private life and scare you about being arrested, etc. They can tell anything to achieve their ends. For example, my mother received a call about a child in distress, but it was fake. We use internet for anything nowadays but it seems nothing is made to protect people. It really gives me high anxiety everyday…”

“Even if you don’t fall for scammers they waste your precious time.”

“Honestly, the only thing about it is that everyone thinks that they’re not dumb enough to fall for these scams, but we all have our off days where anything seems believable, especially when we are young.”

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

The survey among the participants was done from July – September 2023. 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