feedzai

The State of Scams in the United States of America

GASA
Global Anti-Scam Alliance

23% of Americans fall victim to scams as $159 billion stolen in the last 12 months

In the vibrant yet virtual expanse of America, a creeping shadow has taken hold, a shadow shaped by the relentless increase in deception and theft. TheGlobal Anti-Scam Alliance (GASA) and Feedzai together to unfurl the complex web of scams that casts a pall over American life in their comprehensive State of Scams Report. In the latest chronicle, 2,500 Americans shared their experiences, creating a narrative that traverses the vast American landscape.

The story unfolds with an eye-opening figure: an overwhelming 73% of Americans reported encountering scam attempts at least once monthly. This barrage of deception was incessant, with a significant number facing scams multiple times a week and an alarming 15% finding themselves in the crosshairs daily. As if woven into the very fabric of society, 57% noted an uptick in such fraudulent encounters over the past year.

Scammers, like unrelenting rain wearing away at stone, exploited every channel available to breach the day-to-day of the American populace. Emails and phone calls were their prime instruments, abetted by Text/SMS and social media platforms, weaving their way into the very fabric of digital communication. Gmail and Facebook emerged as the principal arenas for these scammers, drawing in half of all reported scam traffic, with Instagram (22%), Google (18%), and WhatsApp (16%) trailing behind. Even the familiar territories of Amazon were not immune, implicated by 15% of respondents as a channel for fraud.

Yet in the face of this onslaught, the American spirit of resilience shone through, with 69% affirming their confidence in spotting such scams. However, this self-assurance was betrayed by the staggering 89% who admitted to being ensnared by scams or identity theft over the previous year, highlighting the sophisticated guile of the scammers.

Examining the types of scams, Identity Theft was the most devastating, impacting 39% and leaving a trail of destruction in its wake. Shopping Scams lured 35%, baited by the allure of seemingly incredible deals. Other fraudulent schemes were dotted throughout the scam landscape, from Advance Fee fraud to the emotionally manipulative Romance Scams.

As the narrative digs deeper, the impact of these scams is seen to be both deep and wide. Americans collectively bore a financial loss of $159 billion over 12 months, an average of $2,663 per victim, striking a blow to the financial wellbeing of countless individuals.

Beyond the stark financial implications, the emotional toll was just as significant, with over half of the scam victims grappling with the silent yet weighty emotional aftermath. The enticement of irresistible offers was the siren call for 22%, while 42% were blindsided by the meticulously crafted deceits, failing to recognize the facade until too late.

In this tumultuous realm, the act of reporting scams, potentially a lifeline, was sadly underused. A significant 62% did not report their encounters with scams, allowing the cycle of deceit to persist. When probing into this hesitancy, a lack of clarity regarding where to report (32%) and a skepticism about the efficacy of reporting (25%) emerged as key barriers. The government's stance against this scourge received a spectrum of opinions: while 30% recognized their endeavors to combat scams, a slightly larger group, 31%, voiced dissatisfaction, especially concerning the prosecution of scammers.

Drawing this American tale to a close, we see a nation wrestling with the darker aspects of the digital revolution, yet steadfast in hope and tenacity. It stands as a call to arms for collective action, urging both the public and officials to create a unified front against the relentless tide of scams, aiming to build a future anchored in trust and security.

This chapter, representative of the current situation, is not just a mere statistic but a rallying cry, revealing that an astonishing 0.6% of the nation's GDP has been siphoned off by scams. It's a stark reminder that the 23% of individuals who have parted with their money to scammers are more than just numbers — they are a testament to the urgent need for vigilance and collective defense in safeguarding America's digital and financial frontiers.

Jorij Abraham

Jorij Abraham, Managing Director, Global Anti-Scam Alliance

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 3 out of 4 Americans experience a scam on a monthly basis. Unfortunately, 62% of Americans don't report scams to law enforcement because 1) they don't know where to report it, or 2) they don't think it would make a difference. This may have been a result of their previous experiences with reporting scams, where some felt ignored or had their issue downplayed by authorities. Interestingly, 50% of Americans turn to their banks when they fall victim to scams. 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.

Numerous reports from consumers indicate Zelle as a preferred tool of fraudsters because of its easy-to-exploit instant payments. The availability of instant payment means that money can move in minutes or seconds. Once a real-time payment, like those sent through Zelle or FedNow, is submitted, it would be next to impossible to retrieve those funds if they were sent to a scammer. The Office of Senator Warren brought this to the attention of the Banking Committee hearing in 2022 to emphasize that there needs to be stronger regulation in reimbursing and protecting consumers from authorized and unauthorized fraudulent transactions. The CFPB is now considering issuing guidance to push banks to cover fraudulently induced transactions to protect consumers. This is similar to new regulations imposed in the United Kingdom, which dictate both the sending and receiving bank to reimburse scam victims. Americans should look at the UK as a successful case study because their scam losses have fallen by 17% in the past year.

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

Unveiling the Cybercrime Landscape: An Interview with L. Wes Quigley of the FBI IC3

In recent Internet Crime Report by the FBI’s Internet Crime Complaint Center (IC3), the figures show an alarming increase in financial losses due to cybercrime, despite a decrease in the number of complaints. To understand these contrasting trends and delve deeper into the cybercrime landscape, we sit down with **L. Wes Quigley**, who speaks on behalf of the **FBI IC3 unit**. He provides insights into the findings of the report, the evolving threats, and the proactive measures taken by the IC3 to combat these digital dangers.

Mr. Quigley, the last FBI IC3 Internet Crime Report reveals a staggering number of complaints amounting to 800,944, with losses exceeding $10.3 billion. Despite a decrease in complaints by 5%, dollar losses have risen significantly by 49%. How does the FBI IC3 explain these contrasting trends? The contrasting trends can be attributed to the evolving nature of cybercrimes. While there's a decrease in the number of complaints, cyber actors are deploying more sophisticated and high-impact tactics that are leading to higher financial losses. Scams related to investments and cryptocurrencies are examples, where fewer incidents can lead to substantial losses.

Phishing schemes have been identified as the number one crime type with 300,497 complaints. However, the associated dollar loss of $52 million is comparatively small to the $3.3 billion loss from investment fraud. Why is there such a discrepancy, and how is the FBI addressing this? Phishing schemes tend to involve smaller amounts of money per incident, or no loss, but occur at a high frequency. On the other hand, investment fraud often involves larger sums, resulting in a higher total financial loss despite fewer occurrences. The FBI is committed to addressing both by educating the public about the various types of scams and working with law enforcement and private sector partners to investigate and mitigate these threats.

Investment fraud related to cryptocurrency has seen a massive increase, from $907 million in 2021 to $2.57 billion in 2022. How is the FBI adapting to this emerging threat, especially given the anonymity associated with cryptocurrencies? The FBI is continuously adapting its strategies to emerging threats, including cryptocurrency-related fraud. We're working closely with experts in cryptocurrency and blockchain technology to enhance investigative capabilities. Additionally, we are focused on public awareness campaigns to inform people about the risks involved with cryptocurrency investments and provide guidance on how to invest safely.

Can you expand on the work that FBI is doing in partnership with law enforcement and private sector partners to tackle cybercrimes? Certainly! The FBI is fostering collaborations with various law enforcement agencies and private sector entities. By sharing information and insights, we can stay ahead of cybercriminal trends and develop more effective strategies for preventing cybercrimes and assisting victims. Our partnerships are crucial for advancing investigations and holding cybercriminals accountable, irrespective of their location.

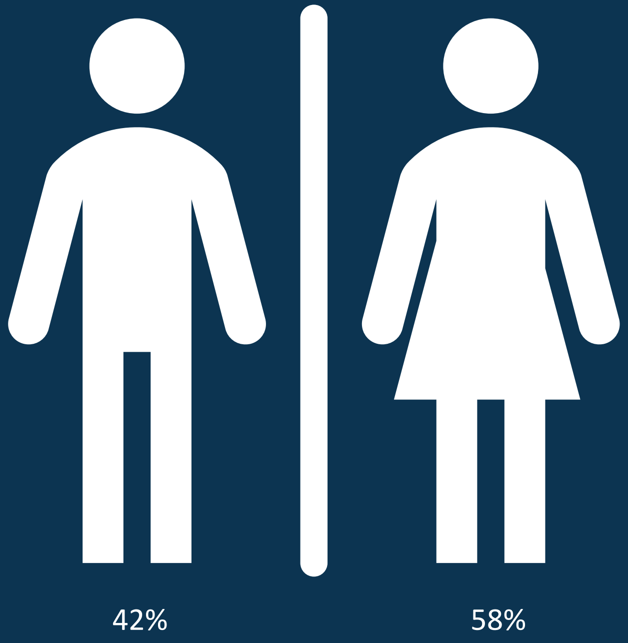
Lastly, considering the escalating cyber threats, what is the FBI’s message to the public, and how can they protect themselves better against these threats? The FBI urges the public to remain vigilant and informed about the various types of cybercrimes and the methods cybercriminals use. We encourage everyone to review consumer and industry alerts published by IC3 regularly. Employing good cyber hygiene practices, such as using strong, unique passwords and enabling two-factor authentication, can provide significant protection. If victimized, it's crucial to report the incident to IC3 and your local FBI field office, as this information is invaluable in tracking, investigating, and mitigating cybercrimes.

The IC3’s unwavering commitment to facing these cyber threats head-on, by working closely with law enforcement, private sector partners, and the public, provides a beacon of hope and reassurance in these technologically turbulent times.

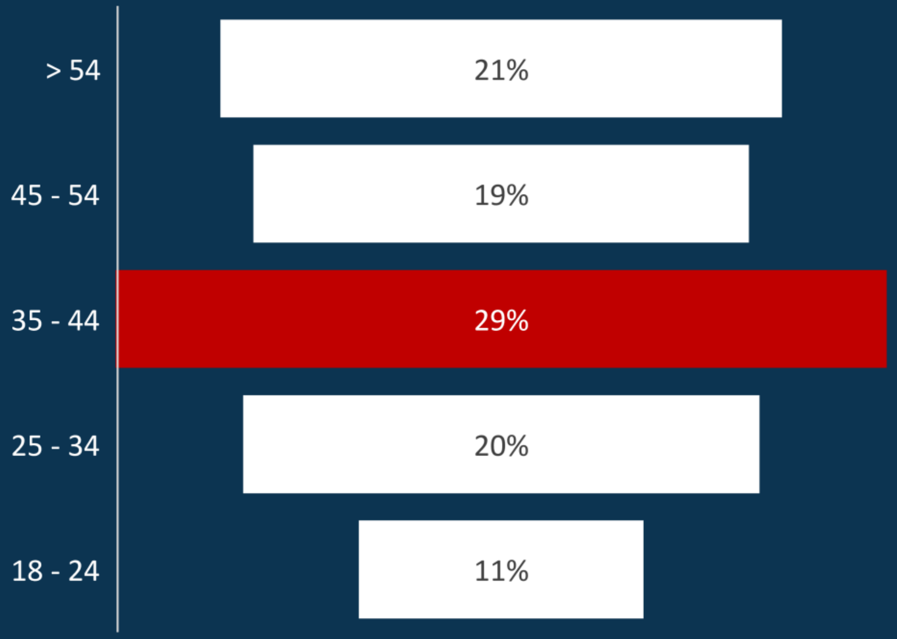
L. Wes Quigley
UC, Internet Crime Complaint Center (IC3),
Federal Bureau of Investigation (FBI)

2,500 Americans participated in the survey

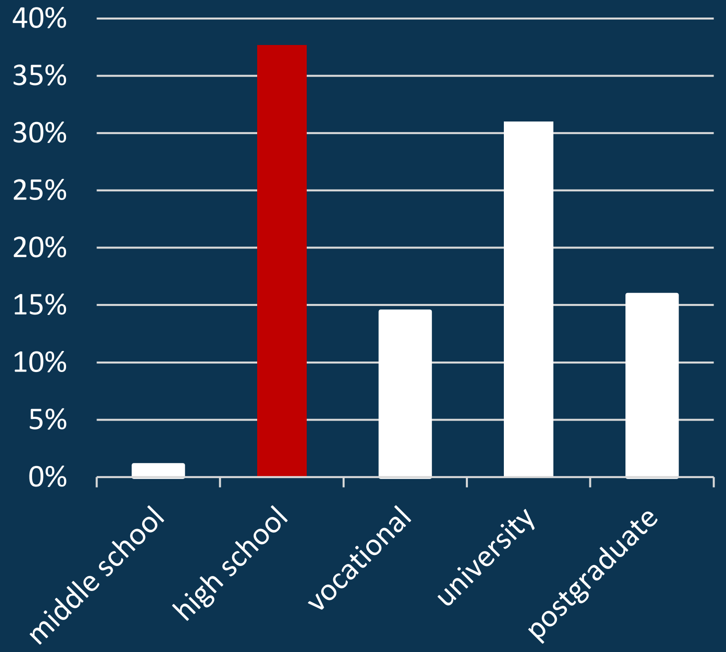
Gender



Age

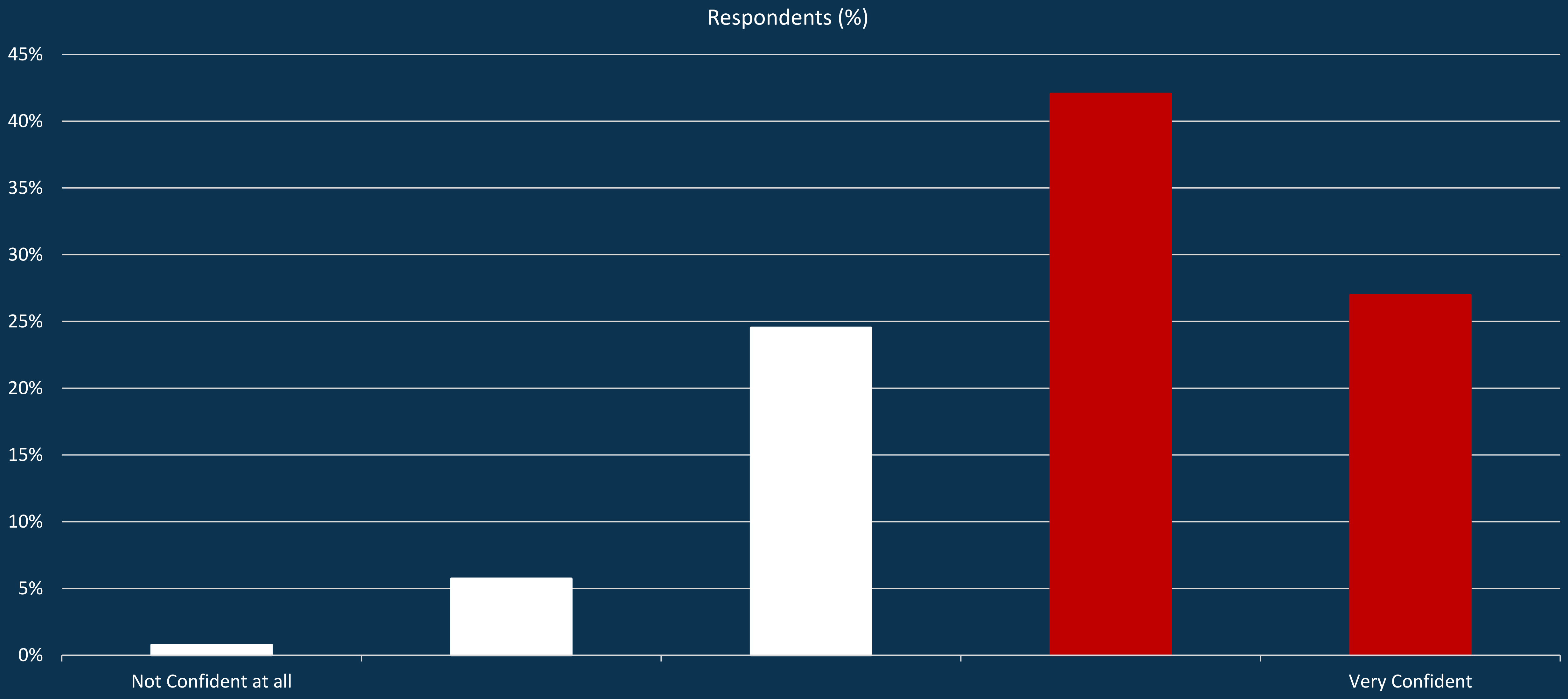


Education



More women than men participated, mainly in the age groups 25 – 44 with a High School education.

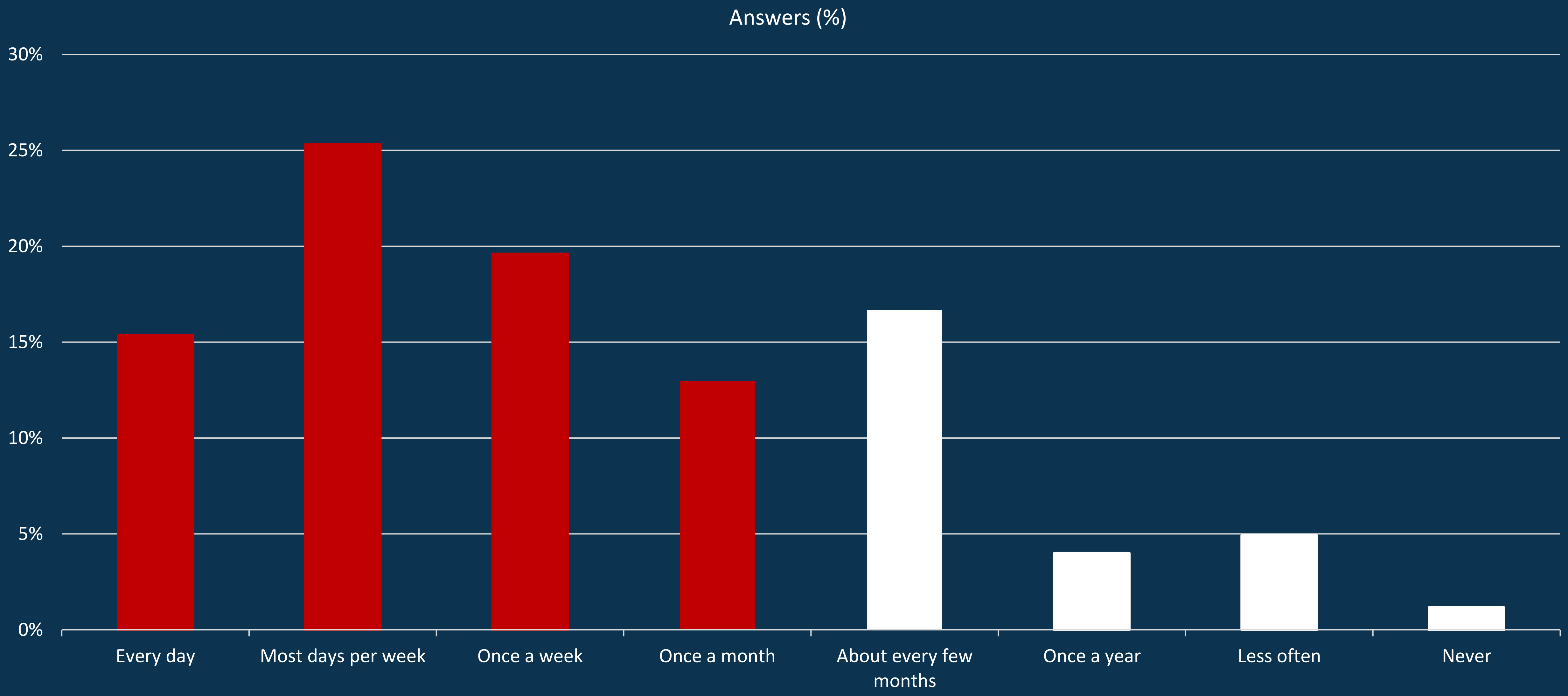
69% of Americans are (very) confident that they can recognize scams



Only 3% are not (very) confident at all.

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

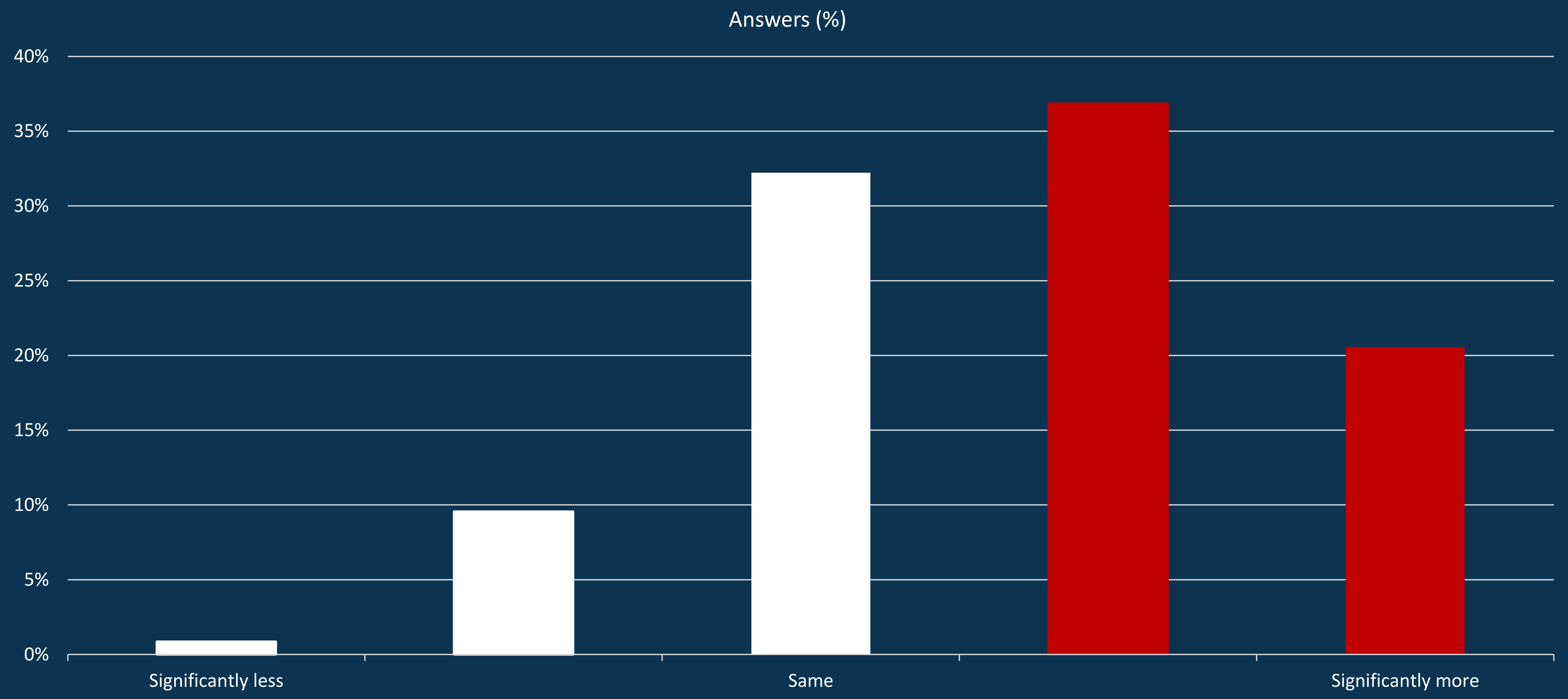
73% of American respondents encounter a scam at least once per month



17% experienced 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)?

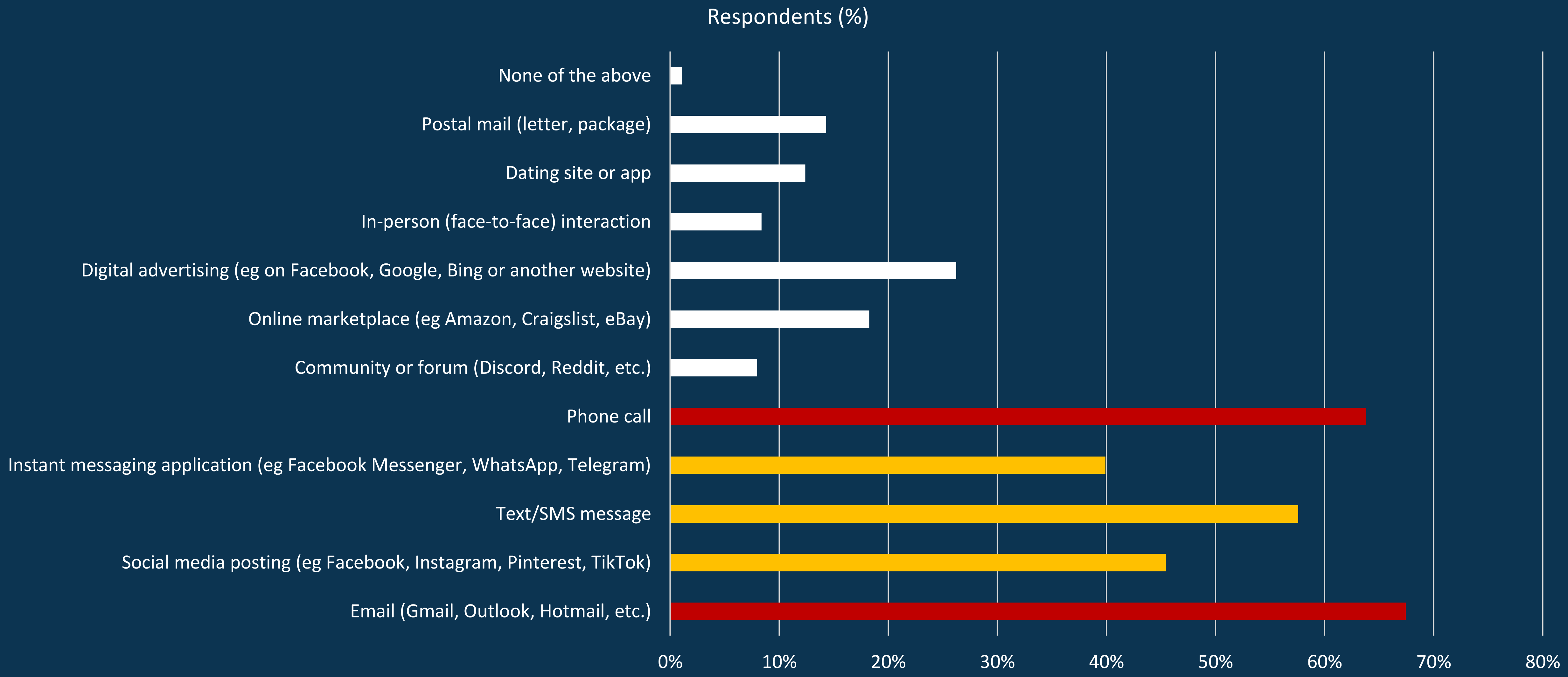
57% of Americans experienced more scams in the last 12 months



Only 10% 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?

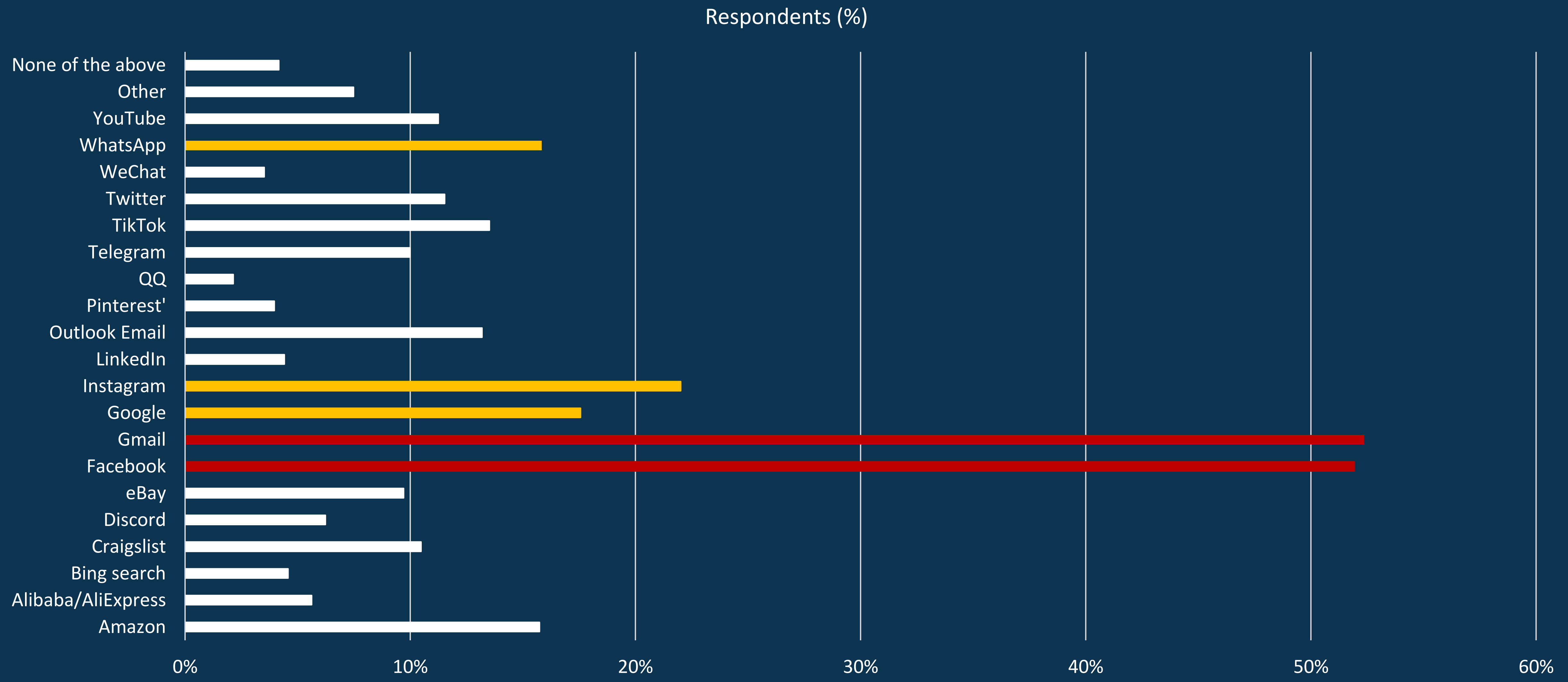
Most Americans receive scams via Email and Phone calls



However, Text/SMS message 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.

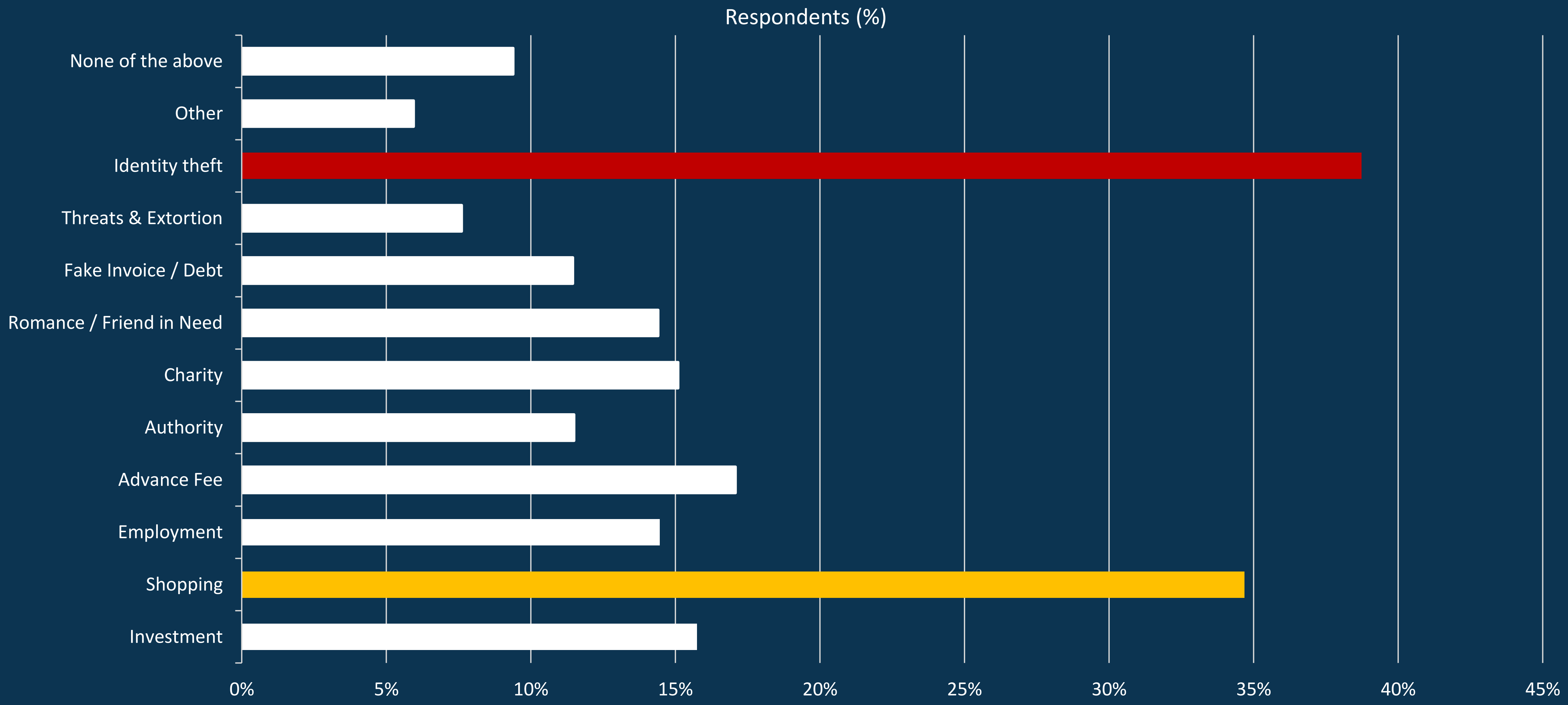
Gmail and Facebook are the most used platforms by scammers in the USA



Instagram, Google, WhatsApp and Amazon take 3rd to 6th place.

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

89% of the participants completing the survey reported losing money in the last 12 months



Identity Theft (39%) and Shopping Scams (35%) are the most common scams in the USA.
Those who were scammed were scammed **twice** on average.

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

Scams are hurting Americans in many ways

“I received an email at work that looked like it was from Intuit QuickBooks saying our subscription was being cancelled for non-payment and I knew I had just paid the bill.

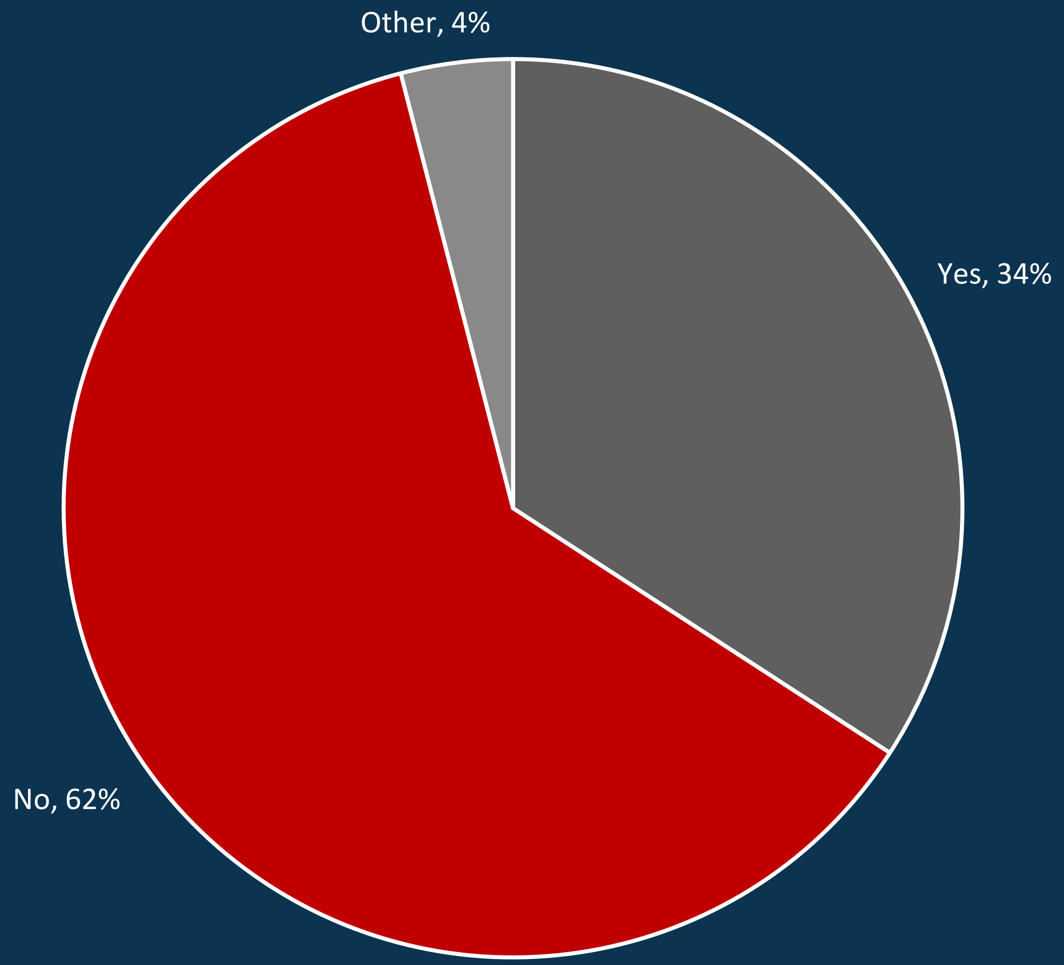
“They pretended that my package was stuck in customs so that I would pay $20 before receiving my items.”

“I was supposed to get a $10 gift card for donating $1 to a political campaign. Donated but never got the gift card.”

“Worked on me for 2 years then started asking money because he needed stuff, and he couldn’t access his account as it had been locked. He professed his love to me and how he was coming to be with me forever.”

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

62% did not report the scam to law enforcement

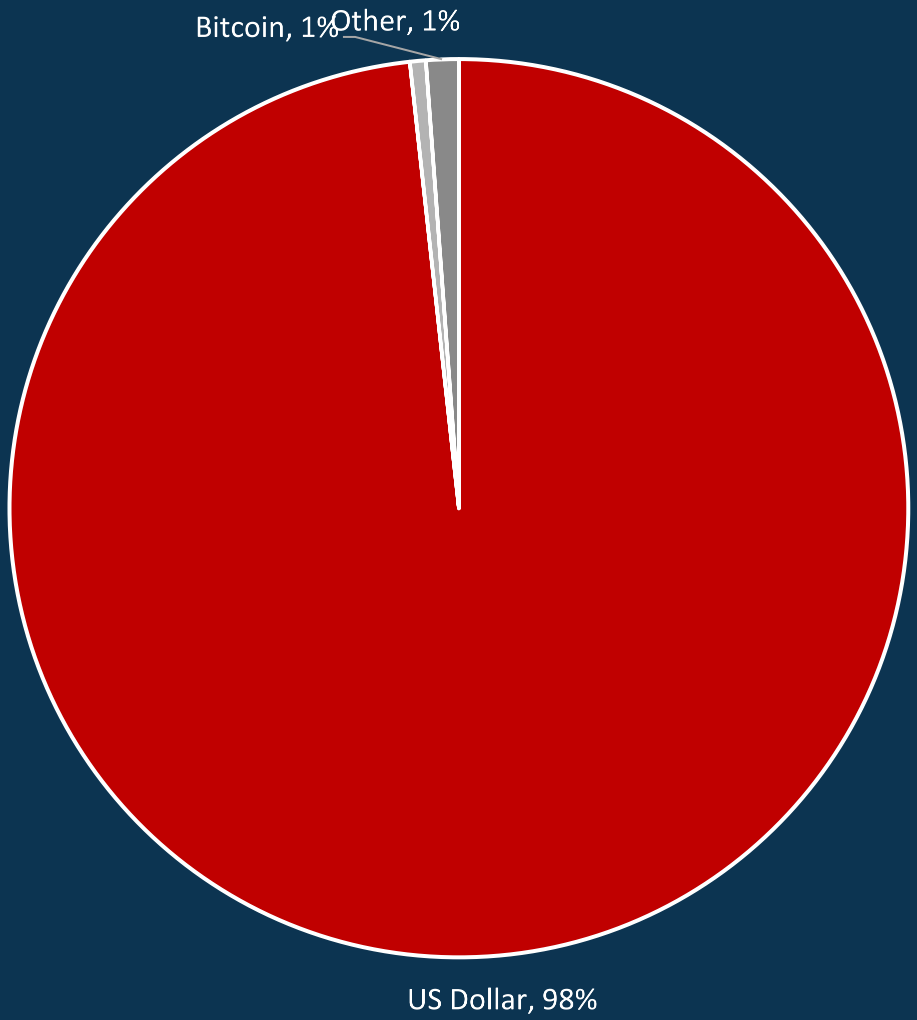


34% stated having reported the scam to law enforcement or another government authority.

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

23% of the approached respondents reported having lost money in a scam last year

Survey Key Statistics	
Number of persons approached	7,556
Participants completing the survey	2,500
Participants losing money	1,703
% losing money / approached persons	23%
Average amount lost in US Dollars	$ 2,663
Total country population	339,665,118
Population over 18 years	265,235,134
# of people scammed > 18 years	59,779,703
Total amount lost in scams*	$ 159,193,348,149
Gross Domestic Product ($ millions)	26,854,700
% of GDP lost in scams	0.6%

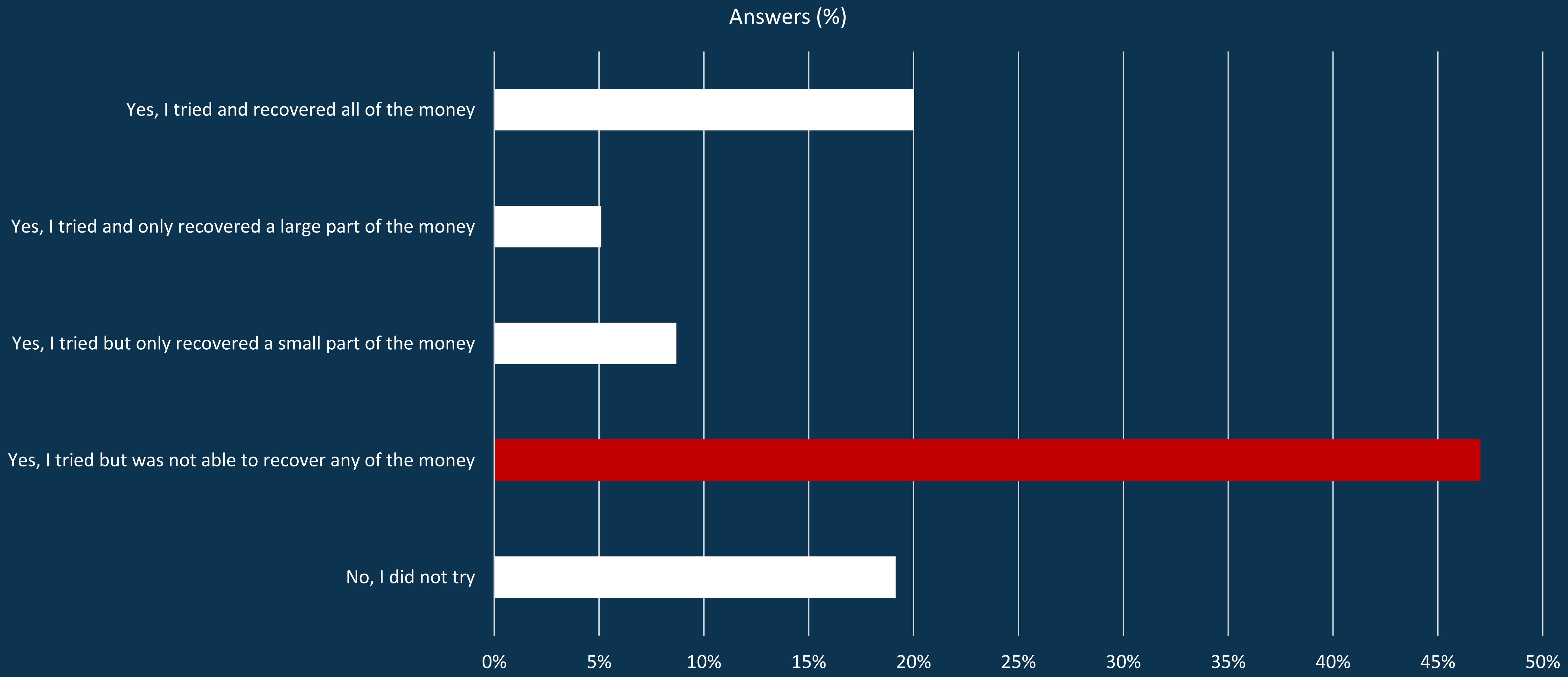


Most respondents report the amount lost in US Dollars (98%), the remainder being Bitcoin (1%) and other currencies

* Bitcoins were excluded from the total amount lost due to an error in the survey questionnaire. One extreme was removed from the answers as well.

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".

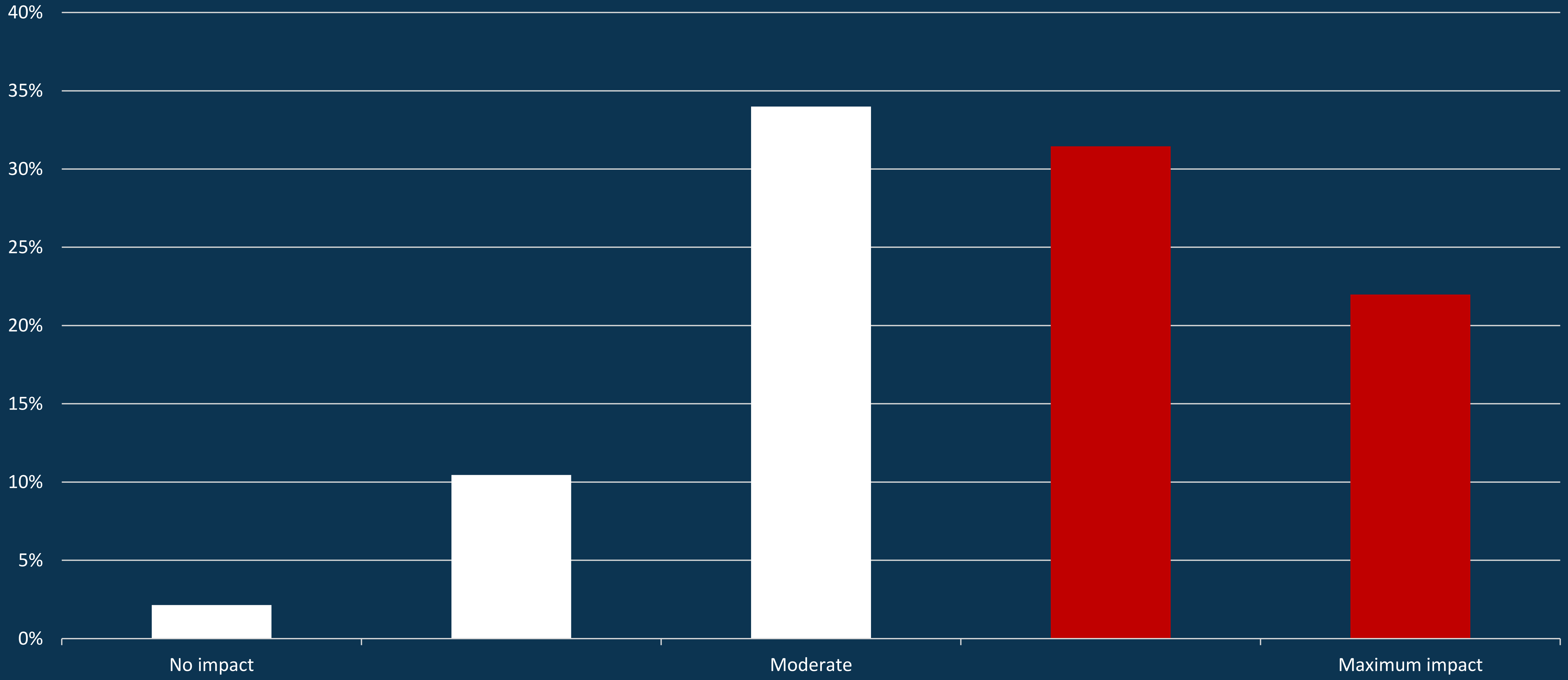
20% of the participants in the survey were able to recover all money lost



19% did not try to recover their funds. 47% tried but was not able to recover any money.

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

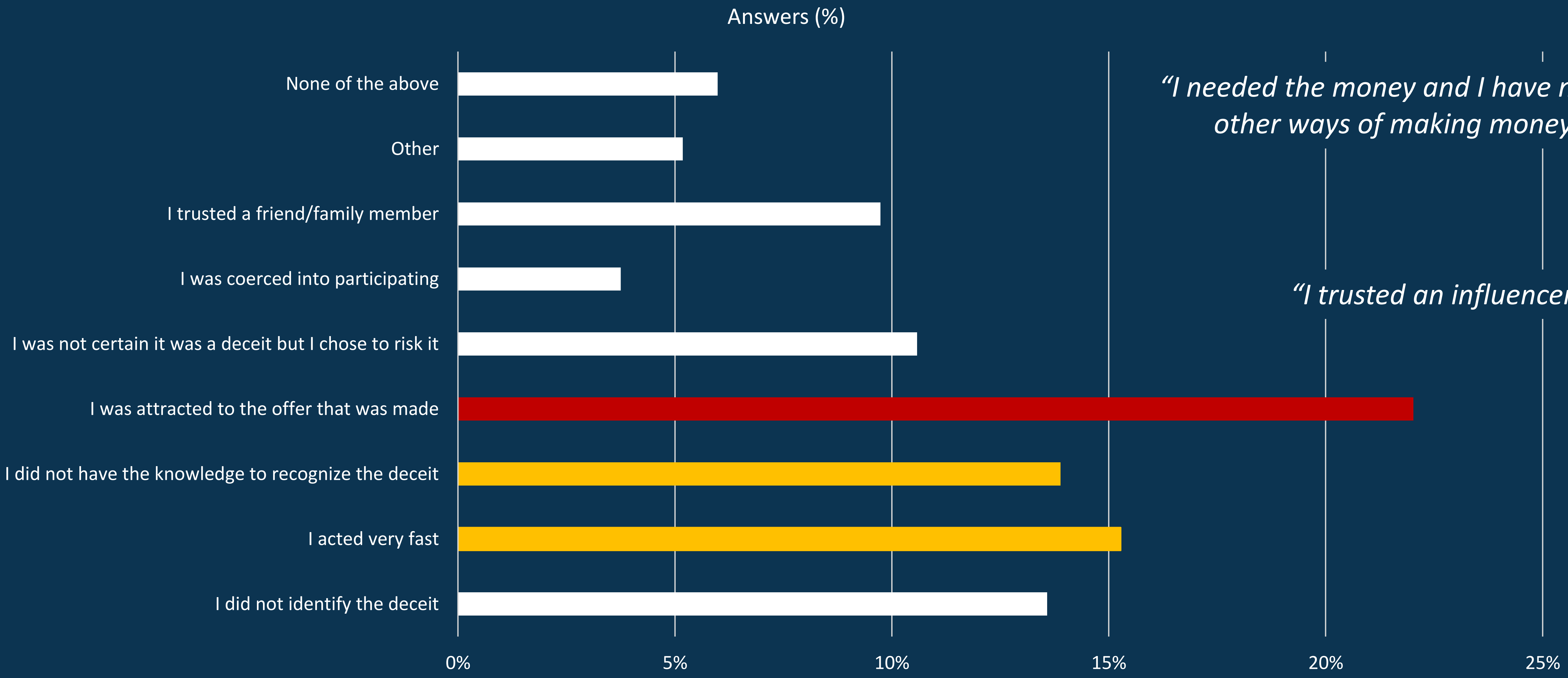
53% of the scam victims perceived a (very) strong emotional impact



13% 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 Americans fall for scams is the attraction of the offer



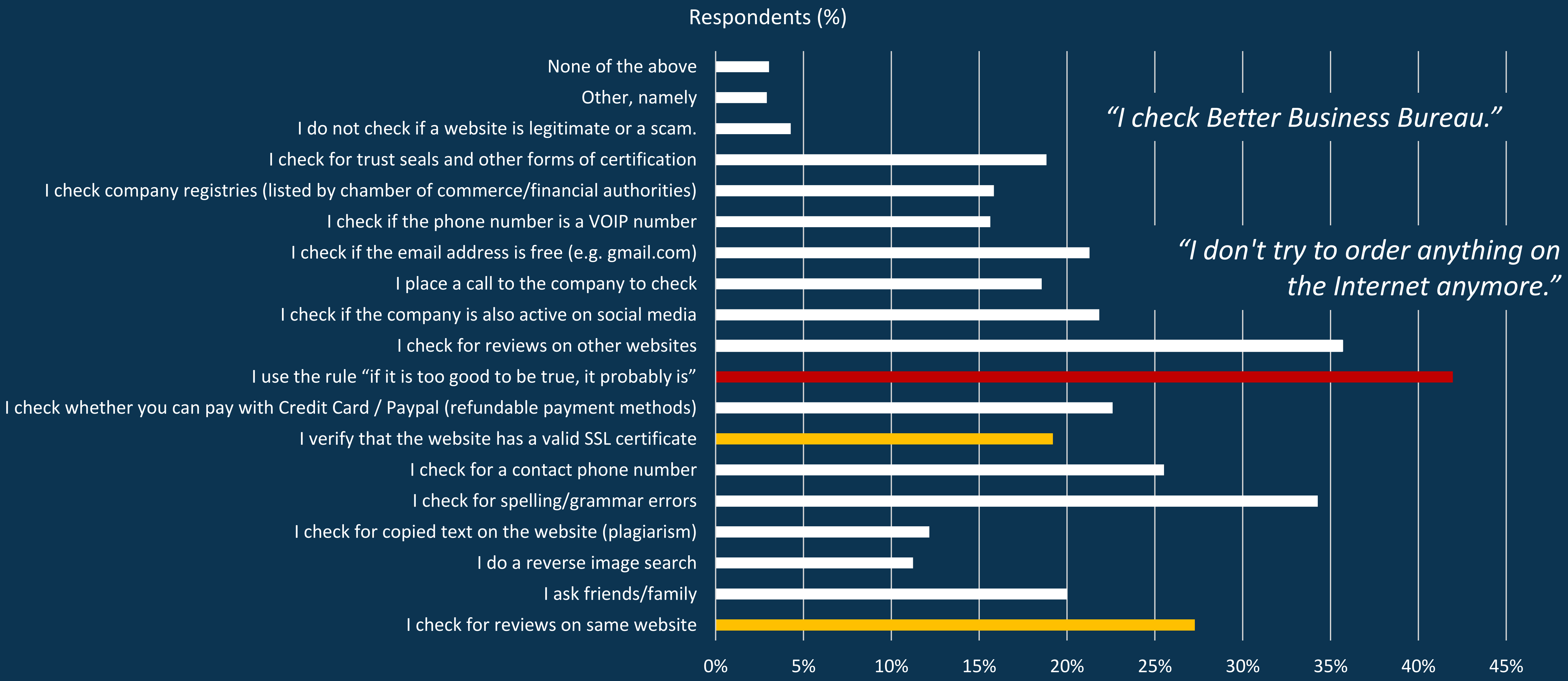
"I needed the money and I have no other ways of making money."

"I trusted an influencer."

Several victims also reported they acted too fast or could not recognize the deceit.

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

The most common way to check for scams is to consider whether it's 'too good to be true'



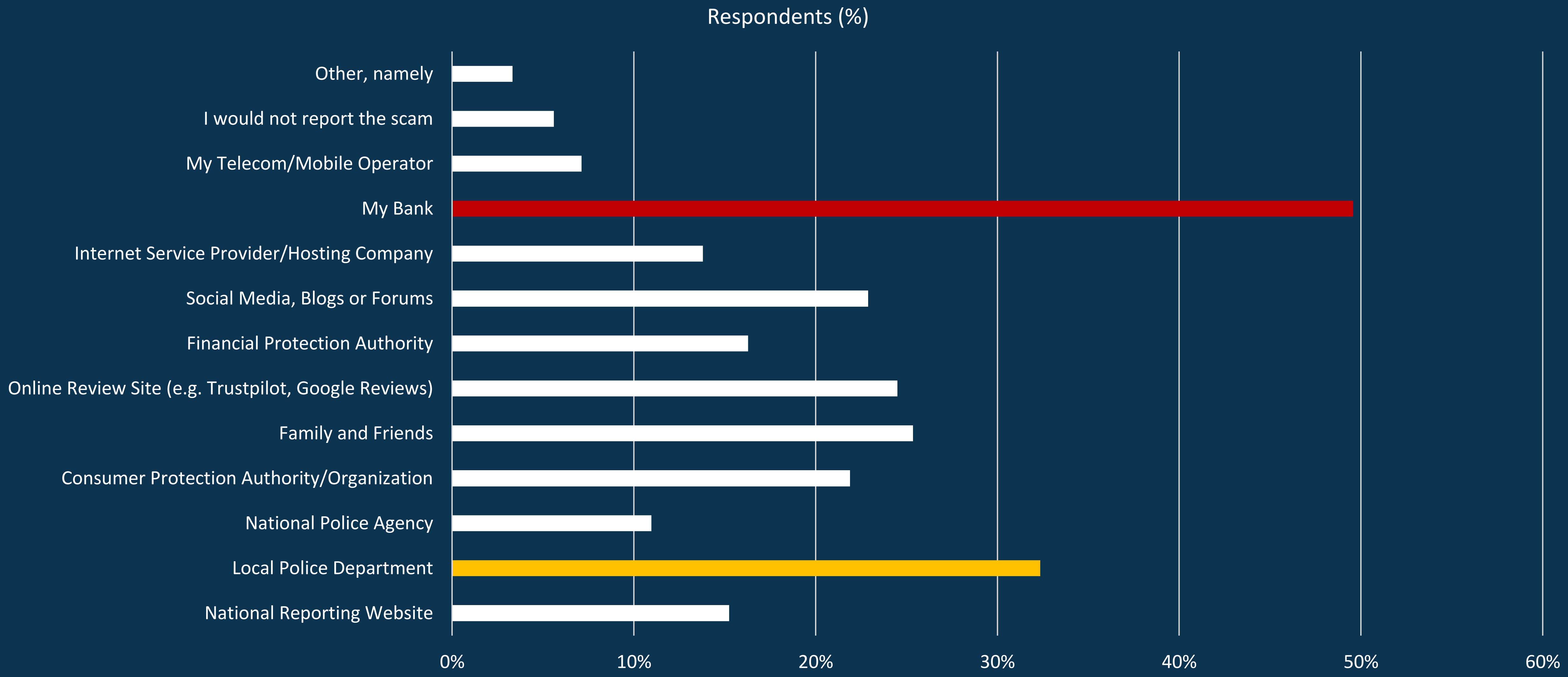
"I check Better Business Bureau."

"I don't try to order anything on the Internet anymore."

Several "unsafe" methods like checking the SSL certificate and reviews on the same site 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.

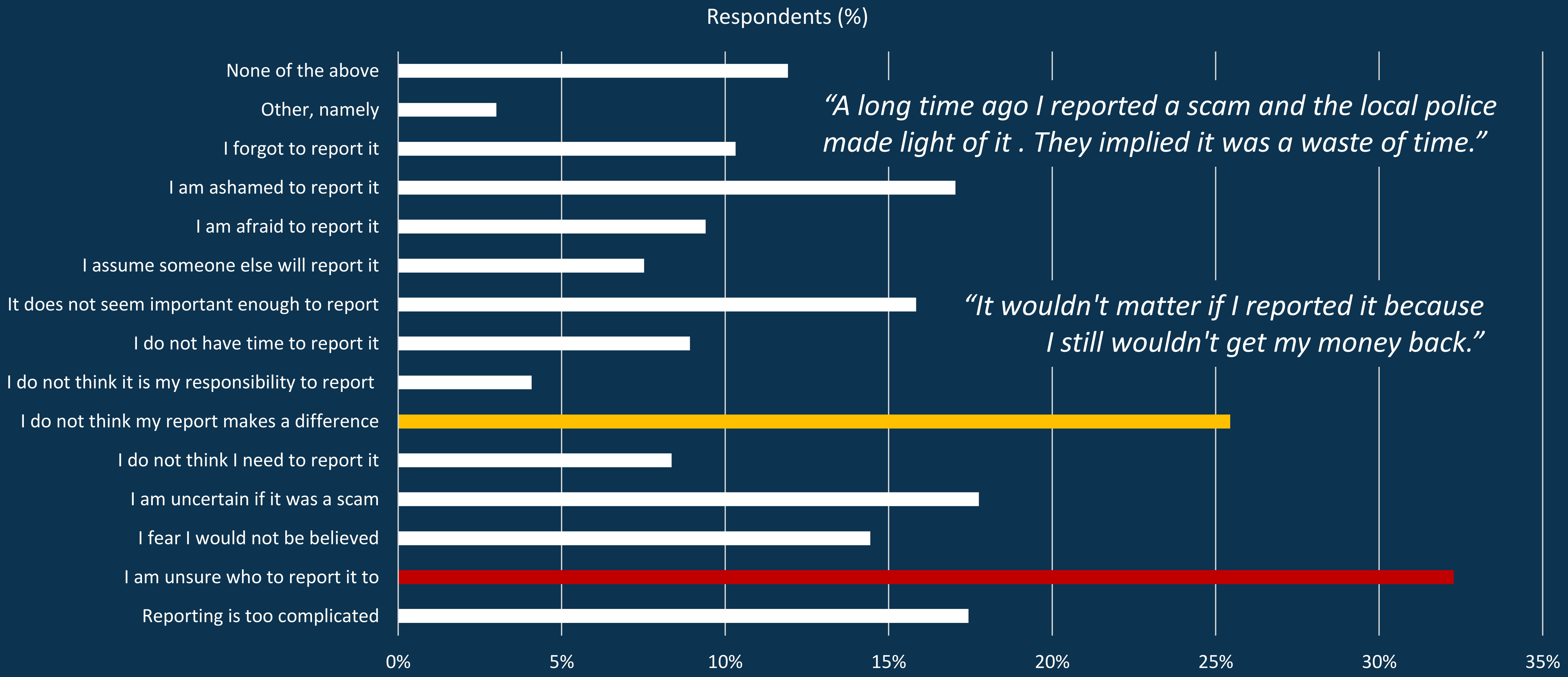
Scams against Americans are mostly reported to Banks



Local Police is also a popular first choice when reporting scams.

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

Scams go unreported as victims are unsure where to report it



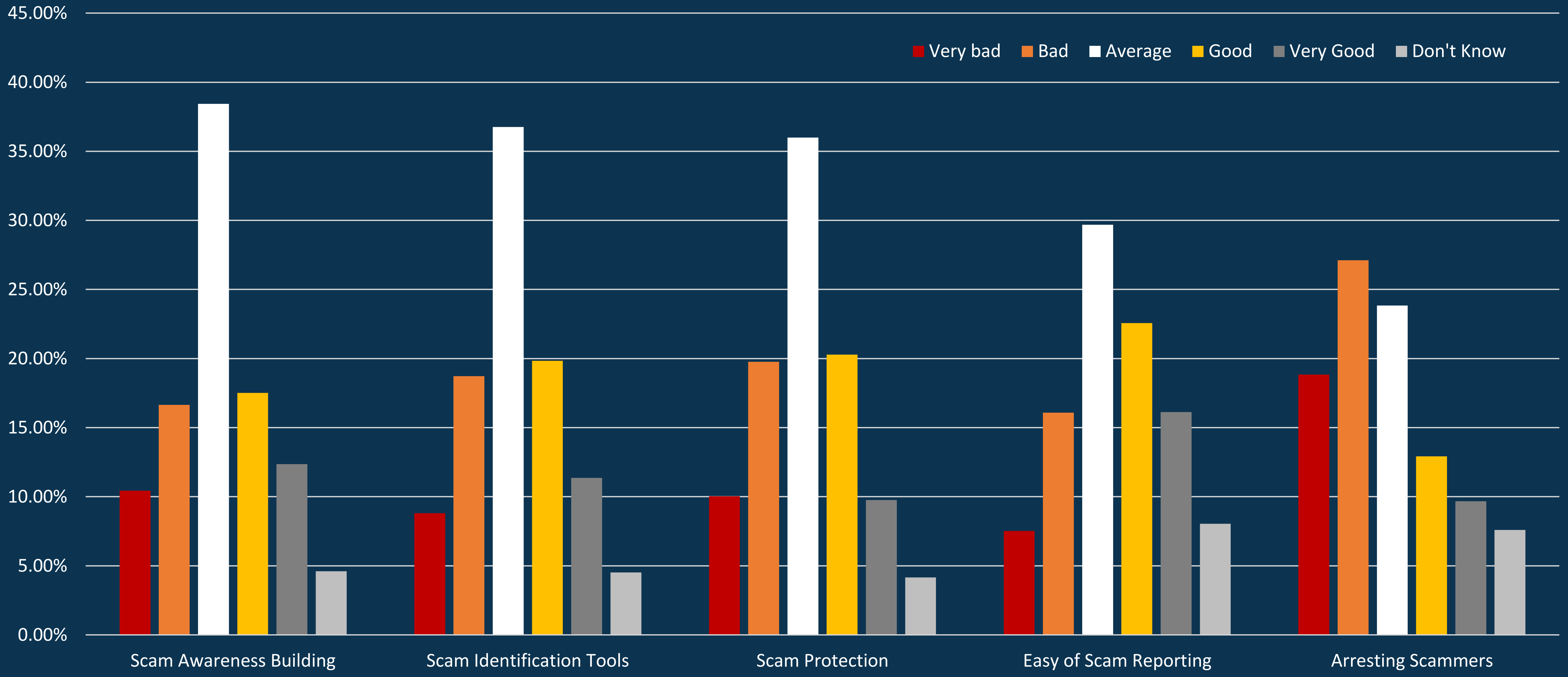
“A long time ago I reported a scam and the local police made light of it . They implied it was a waste of time.”

“It wouldn't matter if I reported it because I still wouldn't get my money back.”

The 2nd more common reason for not reporting are uncertainty about making a difference by reporting.

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

Americans are not pleased about the level of arrests made



Overall, 31% of the participants rate the actions of governments as (very) bad, 30% 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 report scams even though I know the chances of them being caught are slim.”

“The law doesn't go far enough to punish scammers.”

“I wish that people would stop trying to steal hard working people's money.”

“Mostly you get told there is nothing that can be done when you get scammed.”

“Everything that sounds too good to be true is a scam these days.”

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.

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

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.

James Greening, not his real name due to security reasons, is Social Media Manager at ScamAdviser and a scam investigator. He also runs the popular website Fake Website Buster.

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.

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

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