feedzai

The State of Scams in Singapore 2024

GASA
Global Anti-Scam Alliance

Singaporean consumers report landmark progress in battle against scams

The **2024 State of Scams in Singapore** report is a testament to the ongoing commitment of the **Global Anti-Scam Alliance (GASA)** to uncover and analyze the ever-evolving tactics employed by scammers. In collaboration with **Feedzai**, this year's study highlights not only the significant financial and emotional toll of scams on Singaporeans but also the persistent challenges in fighting fraud.

Singapore has long been known for its advanced infrastructure and tech-savvy population. However, as our findings reveal, this same digital interconnectedness has made the country a prime target for increasingly sophisticated scam tactics. With 65% of Singaporeans facing scams at least once per month and 54% reporting a rise in scam encounters over the past year, it is clear that scams are becoming an unwelcome part of daily life for many. The use of artificial intelligence (AI) by fraudsters has further complicated the landscape, making scam detection more challenging and necessitating a coordinated response.

This report uncovers several key trends shaping the scam ecosystem in Singapore. Identity theft remains the most common type of fraud, followed closely by investment and shopping scams. Scammers continue to exploit trusted platforms like WhatsApp, Gmail, and Telegram, with text and SMS scams seeing a 3% increase since 2023.

Alarmingly, 68% of scam victims chose not to report their experience to law enforcement, highlighting a need for more accessible and simplified reporting mechanisms. Additionally, 44% of scams are completed within 24 hours of initial contact, emphasizing the urgency of raising public awareness to help individuals recognize and respond to scams more quickly.

Despite these challenges, Singaporeans show a commendable level of awareness about emerging threats, including AI-driven scams. Most respondents demonstrated knowledge of malicious AI-generated text, chat, and images, though awareness of AI-generated voices and videos remains slightly lower. This indicates progress in educating the public, but further efforts are needed to address gaps in awareness.

The strong response from Singapore's government and financial institutions has also contributed to creating an environment where only 3% of citizens rate anti-scam efforts as poor. Collaborative initiatives between public and private sectors, such as anti-scam apps and reporting platforms, have been pivotal in combating fraud. However, with 55% of Singaporeans reporting diminished trust in the internet due to scams, it's evident that continued efforts are essential to rebuild confidence and ensure a safer online environment.

The findings of this report underscore the importance of vigilance and education in combatting scams. Public awareness campaigns, partnerships between financial institutions and tech companies, and the use of cutting-edge tools like Feedzai's AI-powered risk management platform are critical components in reducing the prevalence of scams and supporting victims. We are committed to fostering such collaborations and equipping individuals with the knowledge they need to protect themselves.

We thank Feedzai for their support and expertise in making this research possible, and we urge policymakers, businesses, and citizens alike to take the findings of this report to heart. By working together, we can build a safer digital ecosystem for everyone.

Sam Rogers
Director of Research and Marketing
Global Anti-Scam Alliance

The Singapore Government adopts a whole-of-society approach in tackling scams

Why does the Singapore government fight scams so hard?

Scams have increased significantly, and have become the main driver of crime.

In 2024 alone, there were over 50,000 reported scam cases – which means roughly 1 in every 100 people in Singapore falling victim. Losses increased by over 70% from the previous year, and exceeded $1 billion for the first time. That is a staggering amount – more than the annual budget of some of our Ministries!

The harms of scams extend far beyond financial losses. The victims may be scarred psychologically and emotionally as well. In some cases, victims even come to the brink of taking their own lives. It is not just the victim who suffers – their family members and loved ones often have to support the victim emotionally and financially through a very difficult period.

Second, despite the safeguards and extensive public education efforts, we see scammers evolving their tactics and exploiting other vulnerabilities. There are two trends that we are concerned about:

First, we observe scammers preying on human emotions and psychology, and exploiting typologies where victims willingly transfer their monies. In 2024, cases involving self-effected transfers accounted for more than 80% of all scams reports and losses. These include government officials impersonation scams, investment scams and internet love scams. These scams are very difficult to deal with because they cannot be addressed purely through technical safeguards or rules.

Second, as we secure traditional communication channels (e.g. phone calls, SMSes), we observe scammers pivoting to online platforms, including social media platforms and messaging apps such as Facebook and Telegram. Telegram, in particular, has emerged as a platform of concern. In 2024, the number of scam cases reported on Telegram close to doubled compared to the previous year.

Finally, as Singapore pursues its vision of a Smart Nation and a digital society, we want to ensure that our citizens and businesses can operate safely in the digital domain and remain confident in digital transactions. Hence, it is important that we continue to enhance security measures to protect them from online risks and harms, even as we reap the benefits of going digital.

Which new measures have been taken over the last few years to protect Singaporeans?

The Singapore Government adopts a whole-of-society approach in tackling scams. We have made significant progress in our fight against scams in 2024.

First, we strengthened our legislation to allow us to take more effective action against scams. In January this year, we operationalised new offences under the Miscellaneous Offences Act 1906 to criminalise the abuse of SIM cards. The Police has commenced arrests and prosecutions under these offences, and will ramp up enforcement in the coming months.

We also operationalised the Online Criminal Harms Act (OCHA) to allow us to deal more effectively with online criminal activity.

The Police is empowered to issue Directions to online service providers, including messaging apps companies, to prevent accounts or content suspected to be involved in scams from interacting with or reaching Singapore users.

We also passed the Protection from Scams Bill in Parliament in early 2025. The Bill empowers the Police to issue Restriction Orders to temporarily restrict the banking transactions of an individual as a last resort, if there is reason to believe that he will make money transfers to a scammer. Given that majority of scams involve self-effected transfers, such powers would be necessary to protect individuals from scams, especially those who are so taken in by the scammers' deceit that they insist on transferring monies to the scammers.

Next, we have enhanced public education efforts by making scam-related channels and resources more accessible to the public.

In 2024, we launched an enhanced version of the ScamShield mobile app, which protects members of the public from scam calls and messages. Through the enhanced app, users can now check if something is a scam from channels such as WhatsApp and Telegram.

We also launched a "1799" helpline, which is a call centre that operates 24/7. The helpline offers members of the public an easy option to check with, whenever they are unsure if a situation they are facing is a scam.

We want ScamShield to be pervasive – whenever in doubt, check with the ScamShield helpline or app. It should be instinctive for everyone. And there is a good chance, if it is a scam, that others would have reported it too. So you can safely disengage from that suspicious call or message, and you would have given us another signal that this is indeed a scam, which the Police can then act on in their enforcement and investigation efforts.

Simply put, the more we verify, the more we can transact confidently, and the higher our chance of winning this fight against scams.

Third, we have boosted our capabilities to enforce against scammers and recover lost proceeds.

We continue to strengthen our partnerships with private stakeholders to combat scams.

Since 2022, staff from six major retail banks are co-located with the Police at the Anti-Scam Command. This allows Police to swiftly trace funds and freeze scam-tainted bank accounts. In 2024, we expanded this initiative to e-commerce platforms, such as Carousell and Shopee. This has enhanced the ability of the Anti-Scam Command to stop scammers in their online operations.

In 2024, the SPF disrupted more than 57,700 mobile lines, more than 40,500 WhatsApp lines, more than 33,600 online monikers and advertisements, and more than 44,900 websites. Just imagine the amount of further damage that could have been caused if these lines or websites were not taken down. This significant increase in disruptions compared to 2023 is made possible through collaborations with major industry stakeholders such as Meta, Carousell, Google and the Telcos.

SPF also participates actively in internationally coordinated operations against scams.

For example, last year, SPF participated in the Operation First Light, which involved more than 70 countries. During the operation, more than 1,100 persons were investigated and over 3,500 bank accounts were frozen in Singapore, leading to the recovery of more than $16.7 million.

There are many other bilateral and multilateral operations and information exchanges that SPF engages in. Scammers and those who enable scams, such as money mules, must know that they cannot hide anywhere, and the law will eventually catch up with them.

Looking back, which solutions proved to be very successful and why? What do you recommend other countries to do to replicate the successes in Singapore?

The fight against scams requires a whole-of-society effort, with public and private stakeholders working together to put in place upstream safeguards and downstream measures to disrupt scammers' operations. There is no silver bullet in the fight against scams. Notwithstanding, we do see several measures that are particularly useful.

For example, the wholesale blocking of international calls spoofing local numbers reduced the number of such spoofed calls from 900 million in 2022, to 4 million in 2024.

The Government also introduced a new single SMS Sender ID, gov.sg, to be used by all government agencies. Using a single SMS Sender ID makes it easier for the public to identify legitimate SMSes from government agencies. This allows the public to safeguard themselves against government official impersonation scams.

We want to work with industry – including telcos, banks and online platforms – on other needle-moving solutions. Companies have a duty to protect their consumers, by strengthening upstream safeguards to build trusted systems and blocking scammers' access to victims. We have some further ideas in mind which we are discussing with industry, and welcome other proposals that can help strengthen our collective defences against scams.

Beyond strengthening upstream safeguards, we have also found it critical to enhance our capabilities to enforce against scammers and recover lost monies. In particular, the operational model of the Anti-Scam Command, whereby staff from the major retail banks are co-located with the Police, has been effective in the Police's abilities to recover scam proceeds and deprive scammers of their ill-gotten gains. In 2024, the Anti-Scam Command froze more than 21,000 bank accounts and recovered more than $182 million.

If every country has the equivalent of an Anti-Scam Command, whereby prompt interventions can be taken to quickly trace the flow of incoming scam proceeds, and swiftly freeze the bank accounts scammers are using, it will make it more difficult for scammers to access their ill-gotten gains, and decrease their "Returns on Investment".

We sometimes only have minutes or even seconds to trace and stop these transactions before the monies flow out of Singapore. This makes it critical for every country to have a system and processes in place to facilitate cross-border sharing of information, tracing of funds, and freezing of scam-tainted bank accounts.

Mr Sanjay Nanwani
Senior Director
Policy Development Division

MINISTRY OF HOME AFFAIRS

Resilient Together: Building a Stronger Anti-Fraud Future for Singapore

feedzai GASA Global Anti-Scam Alliance

Singapore has long been recognized as a regional leader in detecting and remedying fraud—driven by close public-private collaboration and a willingness to embrace innovative technologies. However, the results outlined in GASA's State of Scams in Singapore 2024 report signal that we must amplify our collective efforts, especially as scammers exploit new and emerging tools such as Generative AI.

With over 1,199 Singaporeans surveyed, it is encouraging to see that 62% still feel confident about identifying scams; yet this has dipped by 6% from last year. Even more concerning is the fact that 68% of attempted scams go unreported—a 20% drop in reporting from a year ago—reflecting the rising normalization of fraudulent activity. Despite more than half of respondents (54%) witnessing an increase in scam attempts over the last year, many still hesitate to involve law enforcement or take necessary steps to protect themselves.

Of special note is the role of phone calls, text messages, and messaging apps such as WhatsApp in delivering scams. With nearly three-quarters of respondents saying they were contacted via WhatsApp, fraudsters are capitalizing on the speed, reach, and intimacy of these channels to connect with potential victims. Adding to the complexity, 38% of respondents reported that AI was used in the scam they encountered, and nearly a third were uncertain whether AI tools were involved at all—underscoring the stealth and sophistication of these new scam vectors.

Financial institutions are at the frontline of this battle. We must acknowledge that detection alone no longer suffices. When scams are completed in under 24 hours, and only 8% of victims manage to recover their losses, the focus must shift towards prevention rather than cure. The latest AI-native technologies now enable banks and payment service providers to spot scams better than their customers. More than 70% of attempted payments to scammers can now be stopped before money ever leaves a customer's account.

Consumers, of course, still have an important role to play: pausing before paying, doing extra research, and forming habits that root out suspicion rather than ignoring it. We are now in the era of GenAI, and it can convincingly mimic voices and draft realistic texts. Simple steps such as performing reverse image searches, verifying web addresses, or making direct phone calls to the source can make all the difference. Again the latest technology can ensure banks provide one smart interaction, tailored warnings at the right time, rather than repeating the same generic warnings which all too rapidly pass unheeded.

Singapore is an excellent example of how concerted cooperation can combat fraud—its robust partnerships between government agencies, financial institutions, telecoms, and technology providers are a global model. I saw this first hand during my visit to the Singapore Anti-Scam Command during the Global Anti-Scam Summit Asia 2024. However, the opportunity exists to take this coordination further. When a scammer's IP address or digital fingerprint is flagged, that information should be shared throughout the entire scam lifecycle. Only by working in unison can we stay one step ahead of criminals who innovate relentlessly.

Scams should not be treated as an inevitable side effect of a digital world; they require continual vigilance, advanced technology solutions, and strong collaboration. At Feedzai, we are committed to supporting GASA's vital work to help Singapore's consumers, businesses, and financial institutions prevent scams from taking root in the first place. It is our hope that by combining robust prevention strategies with proactive information sharing, we can keep Singapore at the forefront of global anti-fraud excellence—and make financial crime a risk that scammers simply cannot afford.

Colin Lee
Regional Director, Asia-Pacific
Feedzai

feedzai

Singapore's Fight Against Scams:
A Model for Public-Private Partnerships and Regional Collaboration

feedzai GASA Global Anti-Scam Alliance

In the **GASA Asia State of Scam Report 2024**, there was stark decrease in the average scam loss per scam victim from over US$4,000 per victim to around US$2,500. Furthermore, Singapore was also among the leading economies for recovering scammed funds. There is something positive afoot in Singapore's scam fighting efforts.

The Singapore government is leading the charge in scam fighting with an aggressive public awareness campaign to increase awareness and vigilance, a centralized Anti-Scam Command and recently and recently there was discussions among regulators to empower the police to take pre-emptive measures in authorized scams.

> "We hope to become a valuable platform & community for organizations who have an interest in fighting scams."

The private sector is playing its part as well in what I am confident will be referenced in future as an example of public-private partnerships to solve for a major societal challenge that is scams. Banks under the umbrella of the Association of Banks continue to push out a series of measures to eliminate potential vulnerabilities that scammers could exploit. Banks together with telcos cooperate closely with the Singapore Police Force's (SPF) Anti Scam Command daily by being co-located. Govtech through its network of technology partners continue to secure critical government digital infrastructure and digital utilities such as Singpass which has become ubiquitous. However, despite these efforts, scams continue to form the majority of crime in Singapore.

In the first half of 2024, Singapore recorded 26,587 scam cases, marking a 16.3% increase from the 22,853 cases during the same period in 2023. The tactics of scams continue to evolve, even faster today due to the democratization of Generative AI. There has been a quick shift from unauthorized scams that featured prominently in SPF's top 10 scam types to authorized scams that today are the most common scam types.

Against this backdrop, GASA has provided a platform for industry players across industries to come together to collaborate against scams. Together with Amazon, Mastercard led the set up of the GASA's first local chapter in Singapore in early 2024. Today the chapter boasts global technology companies, local leading companies and universities. One of our first major achievements was to organize the GASA Asia Summit in October 2024 which till date is the largest GASA Summit. The summit was attended by over 800 delegates (in person & online) from law enforcement, government, international organizations, tech companies, banks and NGOs from across Asia. The event was also graced by 2 government Ministers in Singapore which demonstrates the importance of the topic and this platform.

As we complete our first year as a Chapter here in Singapore, we will continue to grow our community. We hope to become a valuable platform & community for organizations who have an interest in fighting scams. In time, we hope to find encourage collaboration between our members to fight scams. As articulated in our theme of the Asia summit, 'It takes a network, to defeat a network'.

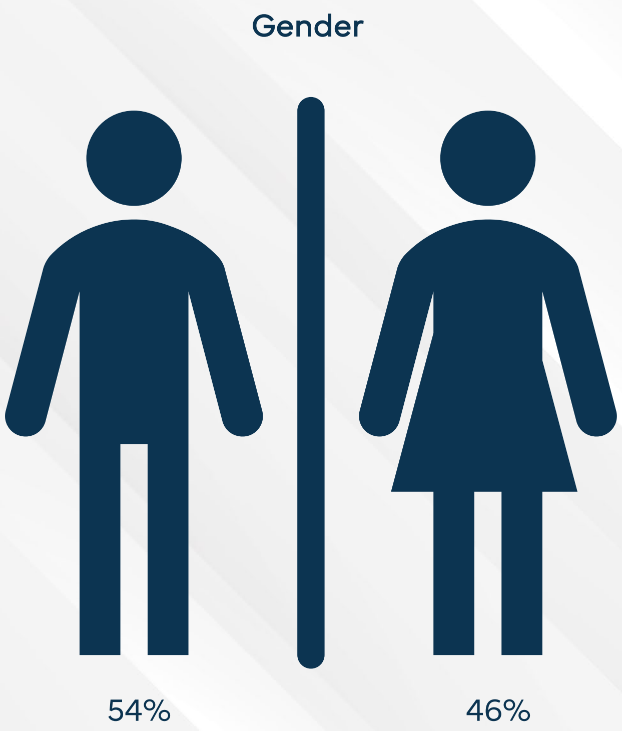
Rajat Maheshwari
Chair
GASA Singapore Chapter

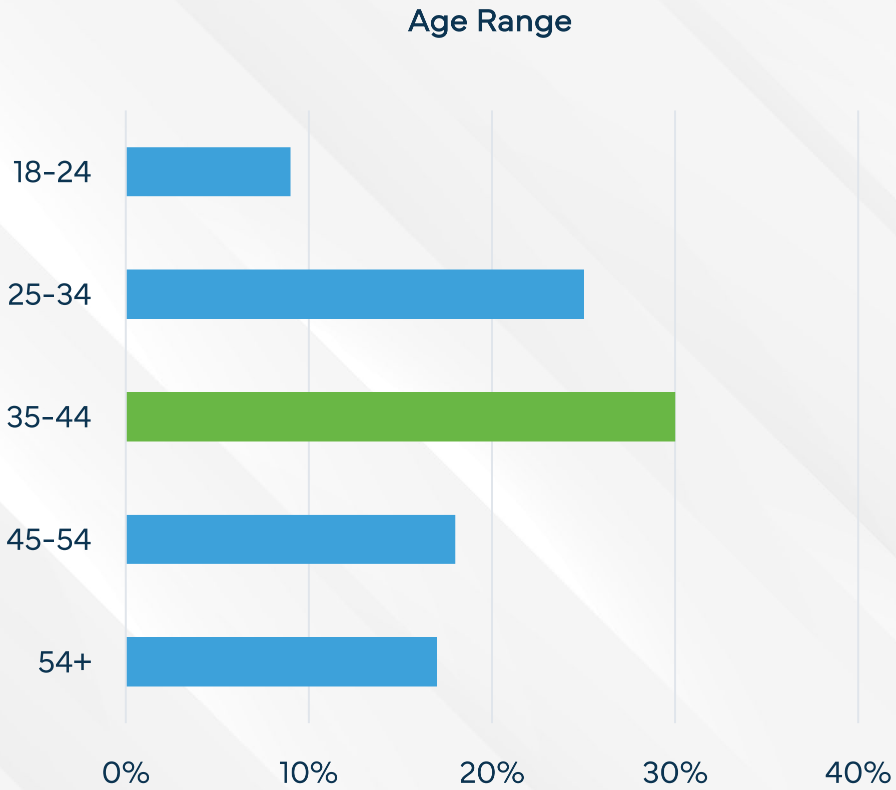
GASA Global Anti-Scam Alliance

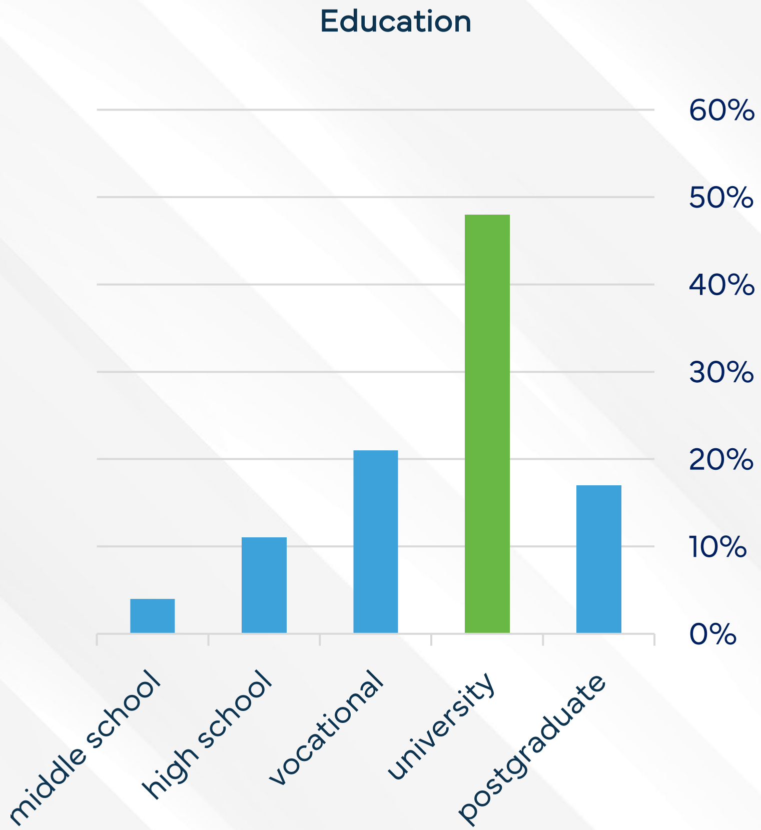
1,199 Singaporeans completed the State of Scams in Singapore survey

feedzai

GASA
Global Anti-Scam Alliance

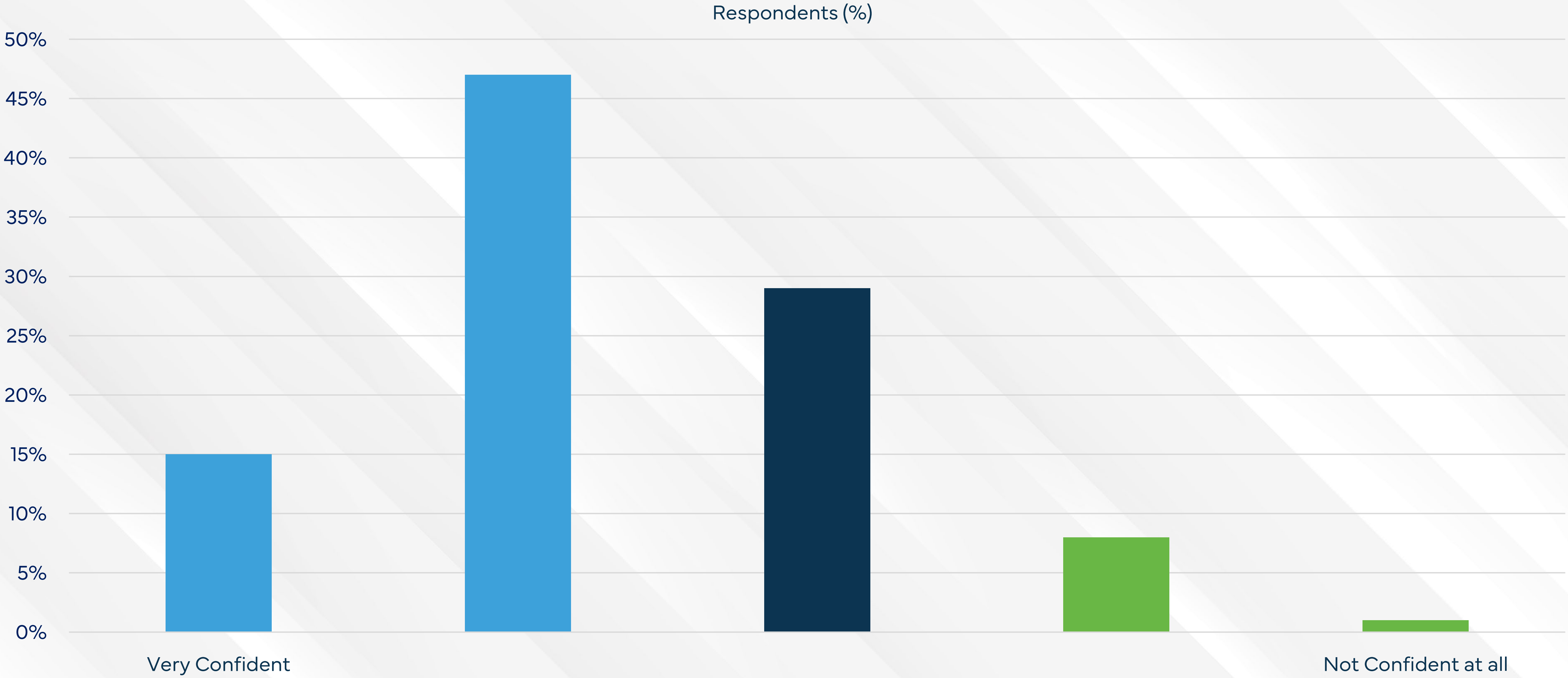






The demography of respondents to the State of Scams in Singapore 2024 survey consists of more men than women. A large proportion were in the 35-44 years age group, with a university degree.

62% of Singaporeans expressed confidence in their ability to recognize scams

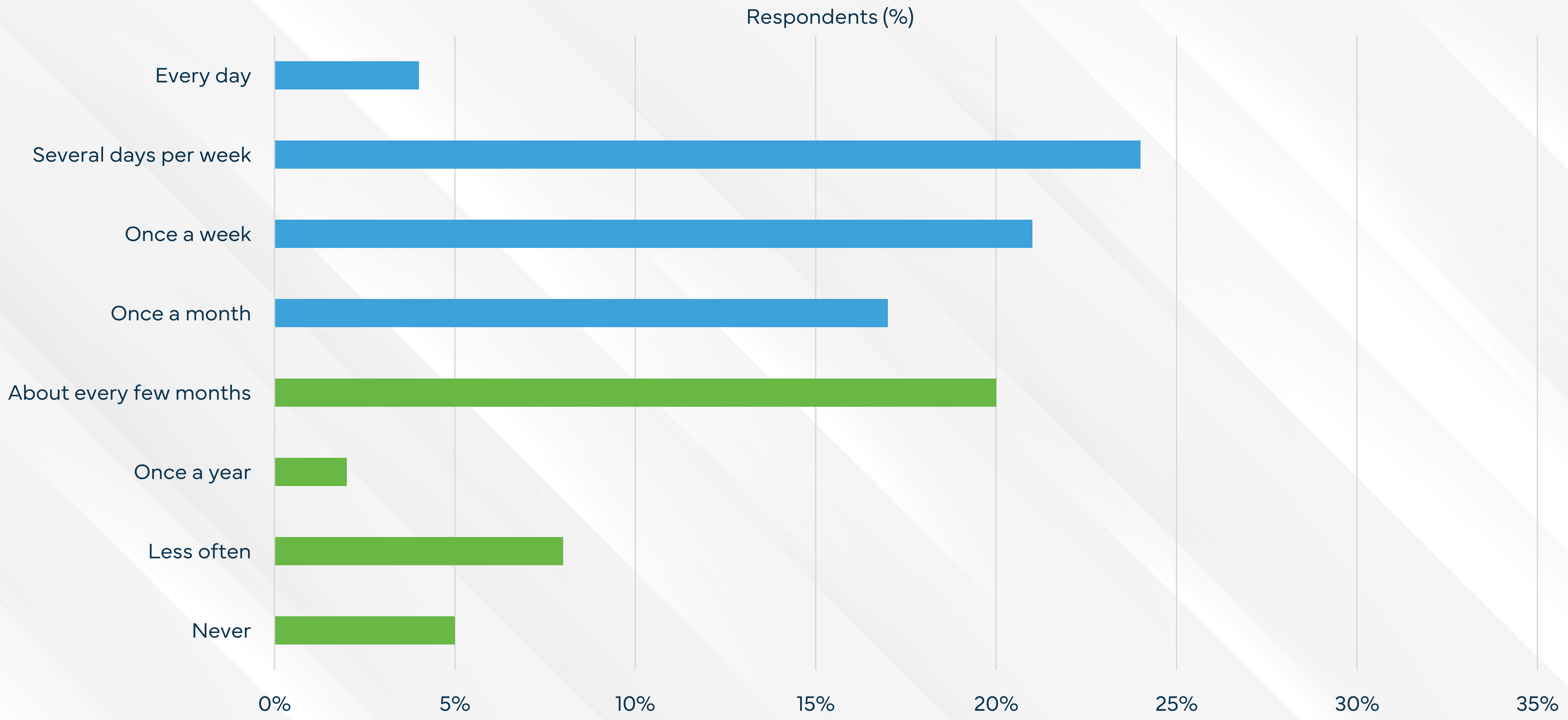


Only 9% of Singapore respondents lack confidence in recognizing scams at all.

Q2 - How confident are you that you can recognize scams?

65% of respondents have encountered scams at least once a month

feedzai GASA Global Anti-Scam Alliance



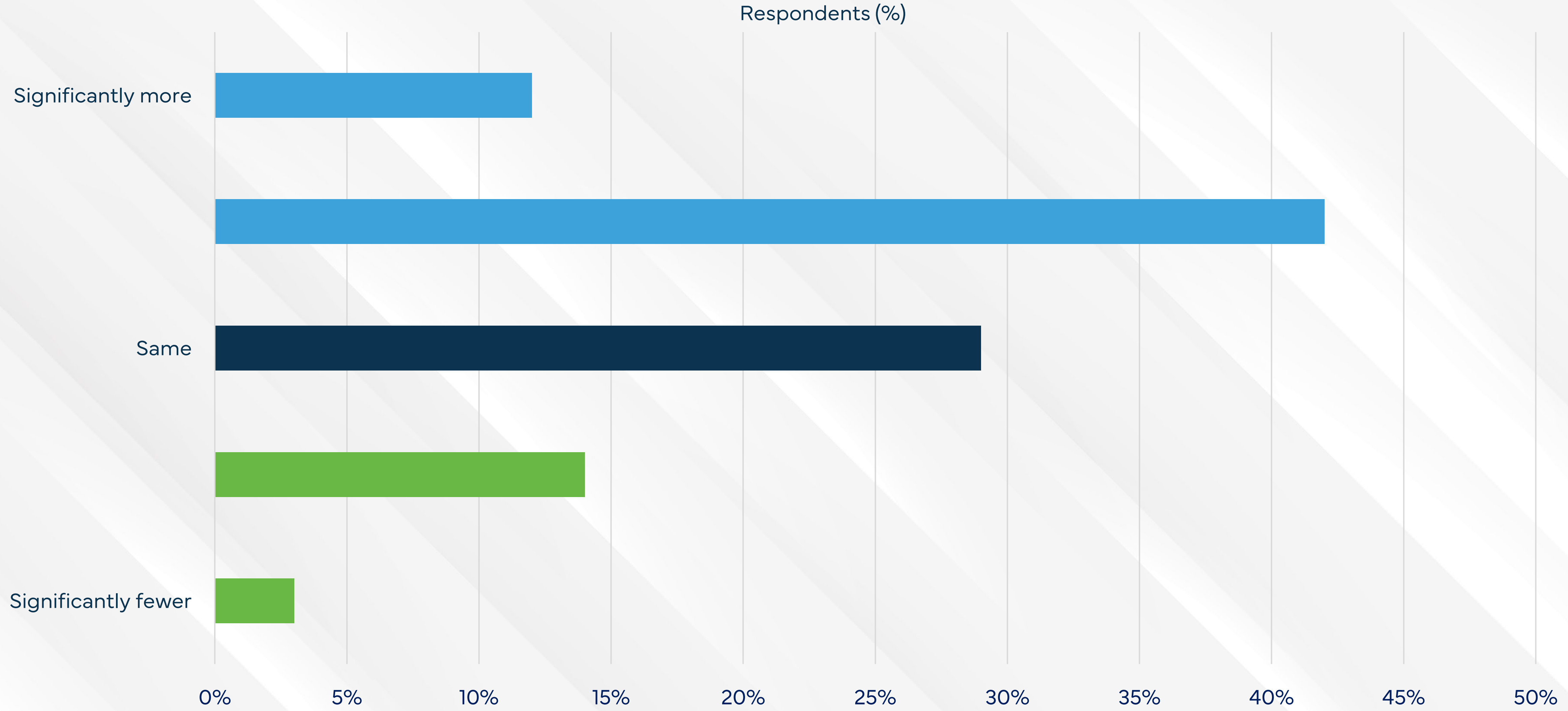
13% of respondents say they do not encounter scams frequently, i.e. less than once a month.

Q3 - In the last 12 months, how often have you been exposed to scam attempts? This includes receiving suspicious content, as well as seeing deceitful advertising.

Compared to the previous year, 54% of Singaporeans felt they have been exposed to scams more frequently

feedzai

GASA
Global Anti-Scam Alliance

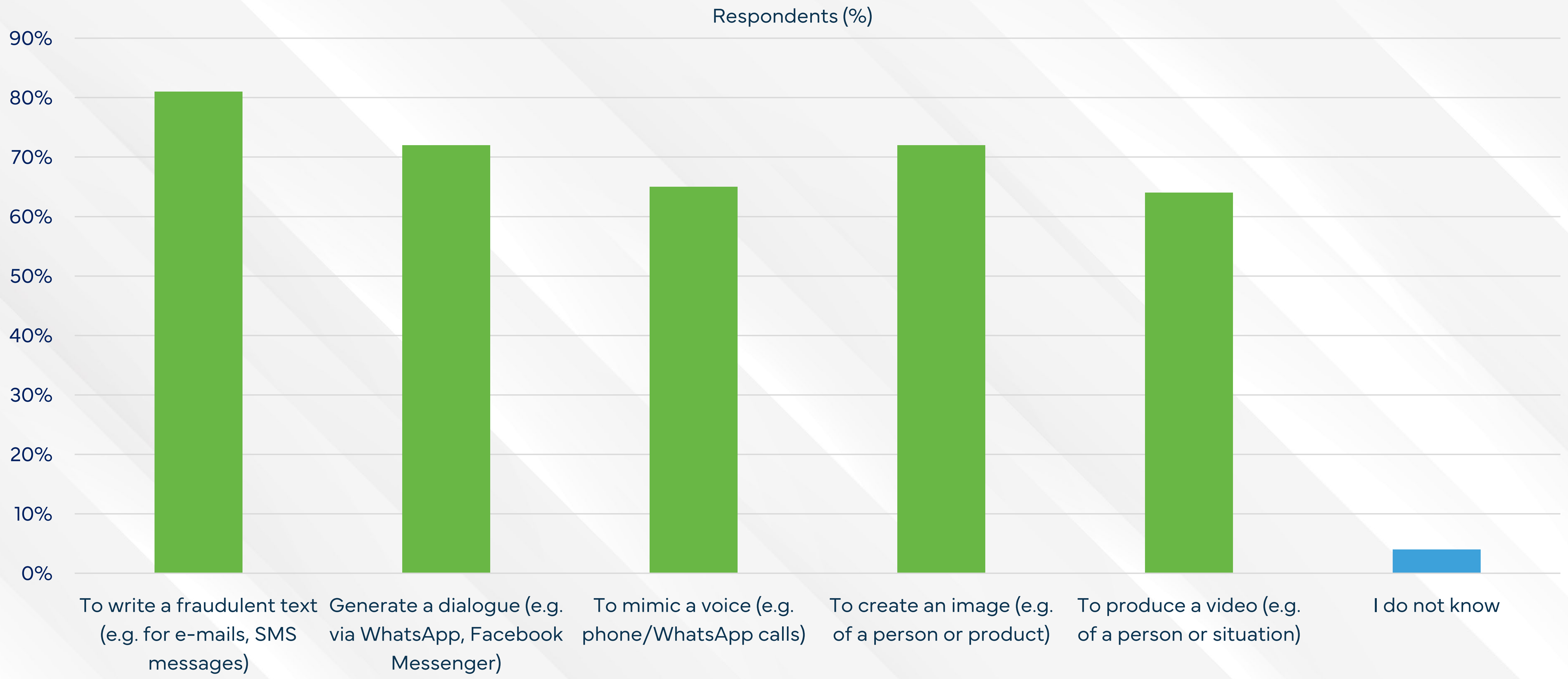


17% of respondents feel that there has been a reduction in their exposure to scams.

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

Most Singaporeans are aware that AI can be used to create malicious content to perpetuate scams

feedzai GASA Global Anti-Scam Alliance

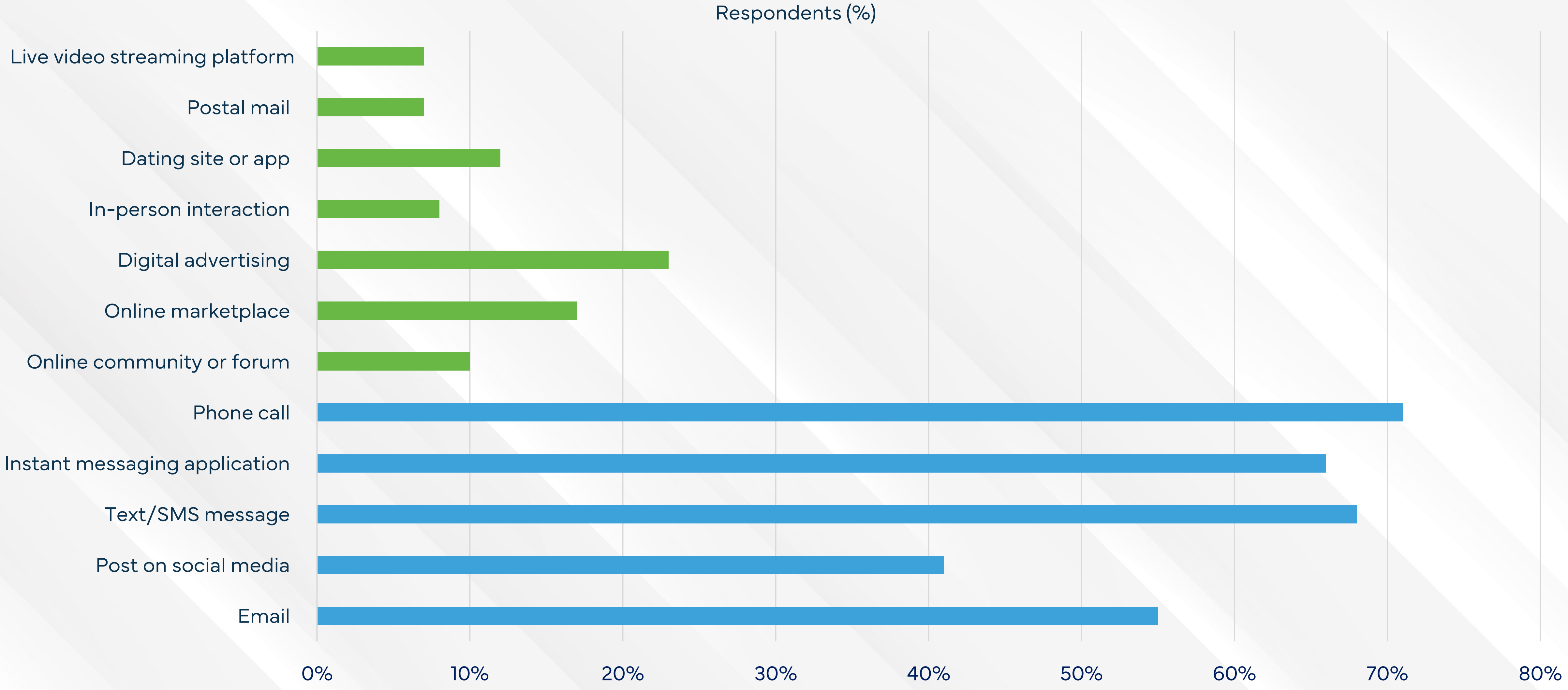


Awareness of the negative effects of AI technology is generally high.

Q5 - For which of the following can Artificial Intelligence (AI) be used?

Respondents say they were approached by scammers through common communication channels

feedzai GASA Global Anti-Scam Alliance



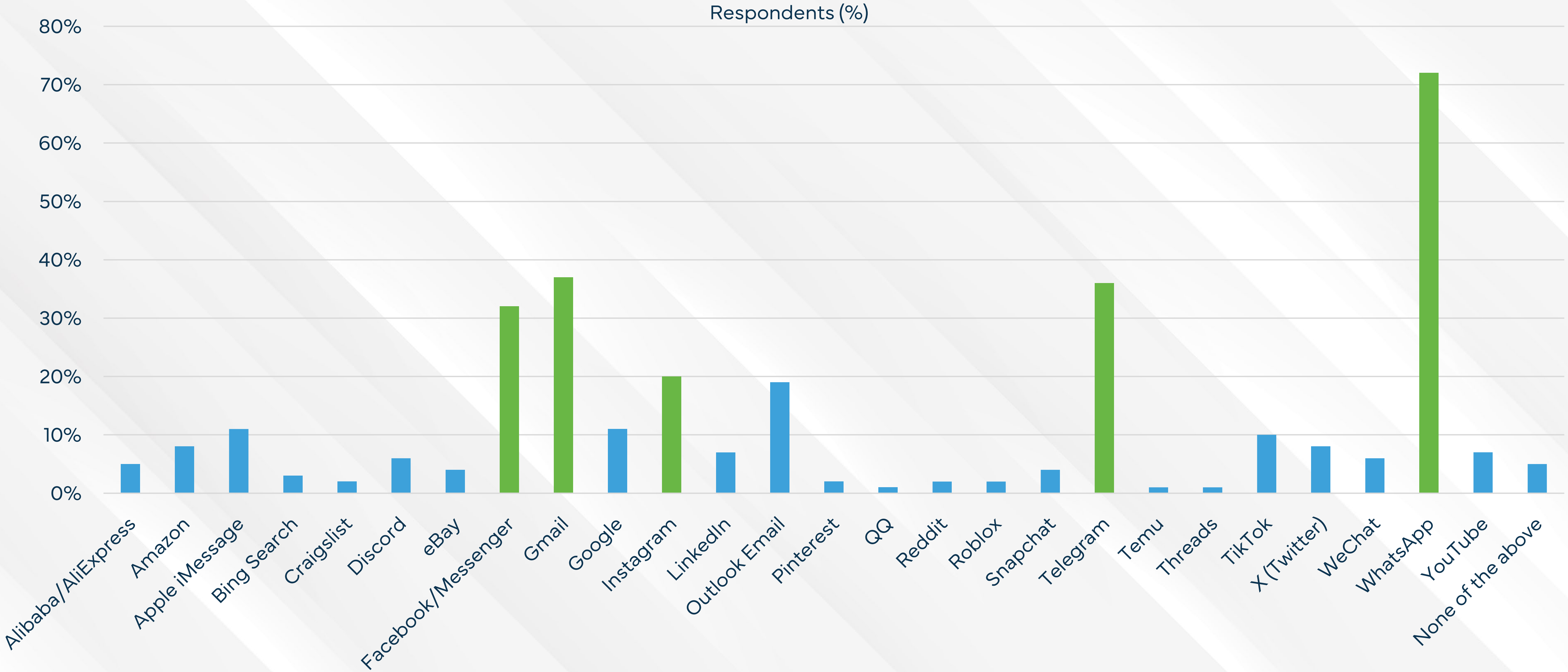
According to respondents, common approach modalities include social media, calls, SMS, and email.

Q6 - Through which communication channel(s) did scammers approach you in the last 12 months?

WhatsApp is the most common online platform scammers use to approach victims

feedzai

GASA Global Anti-Scam Alliance

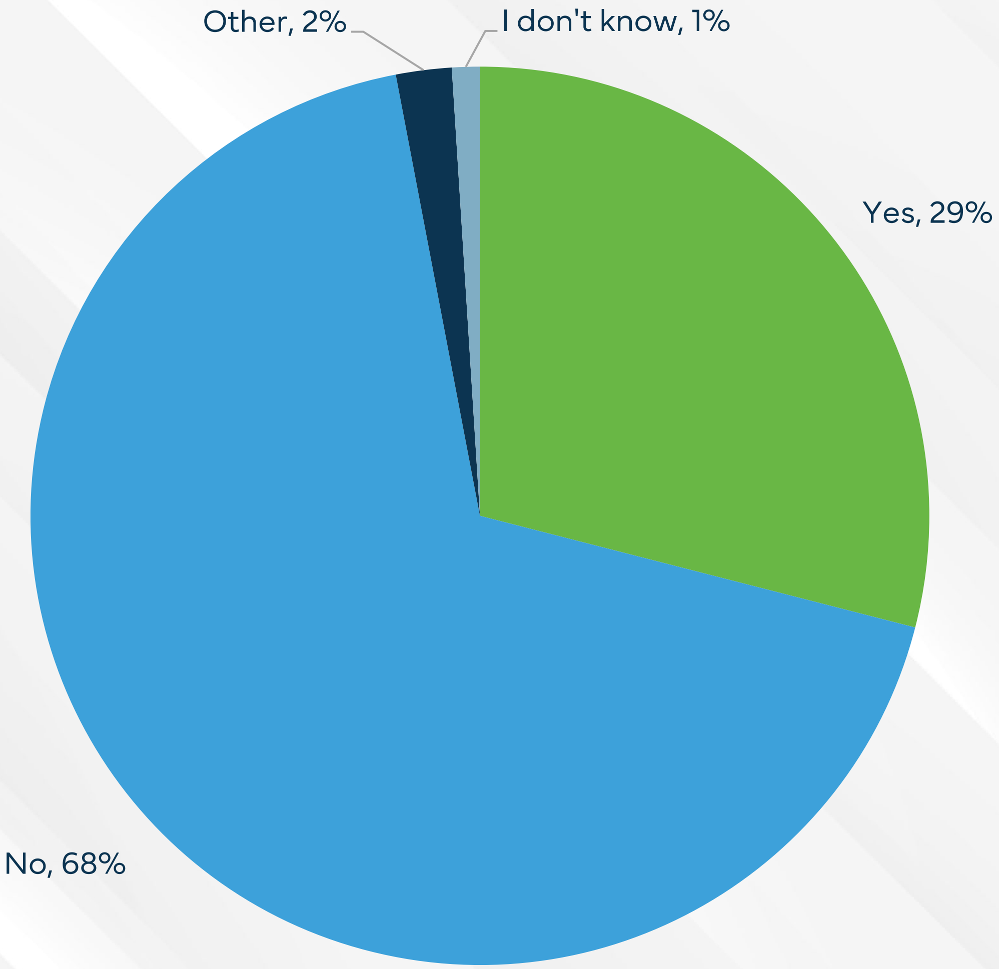


Gmail, Telegram, Facebook and Instagram round out the top five most popular platforms for scammers.

Q7 - Though which platform(s) did scammers contact you in the last 12 months?

68% of Singaporeans did not report their scam or scam attempt to law enforcement

feedzai GASA Global Anti-Scam Alliance



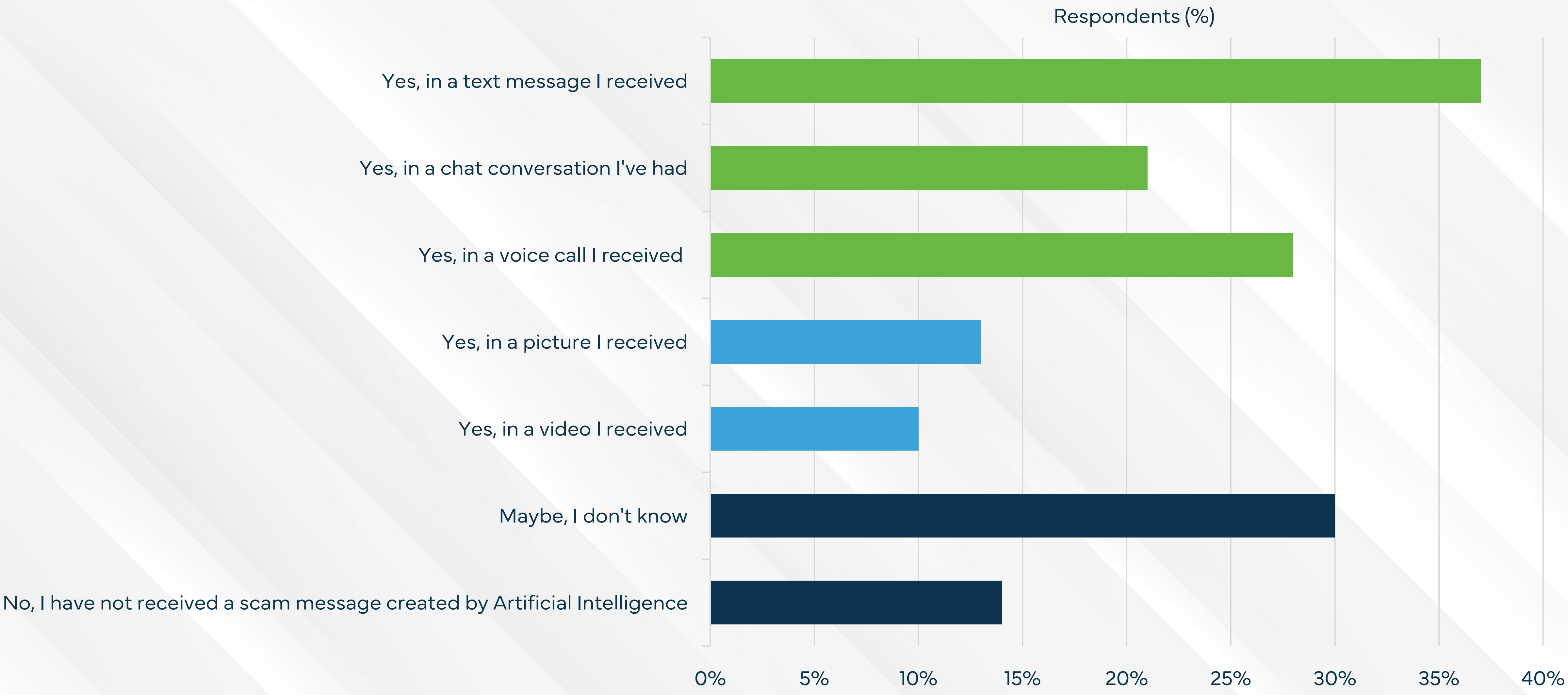
20%

decrease
in reports to law
enforcement,
since 2023

29% stated having reported the scam to law enforcement or another government authority.

Q8 - Did you report a scam or scam attempt to the police or authorities in the last 12 months?

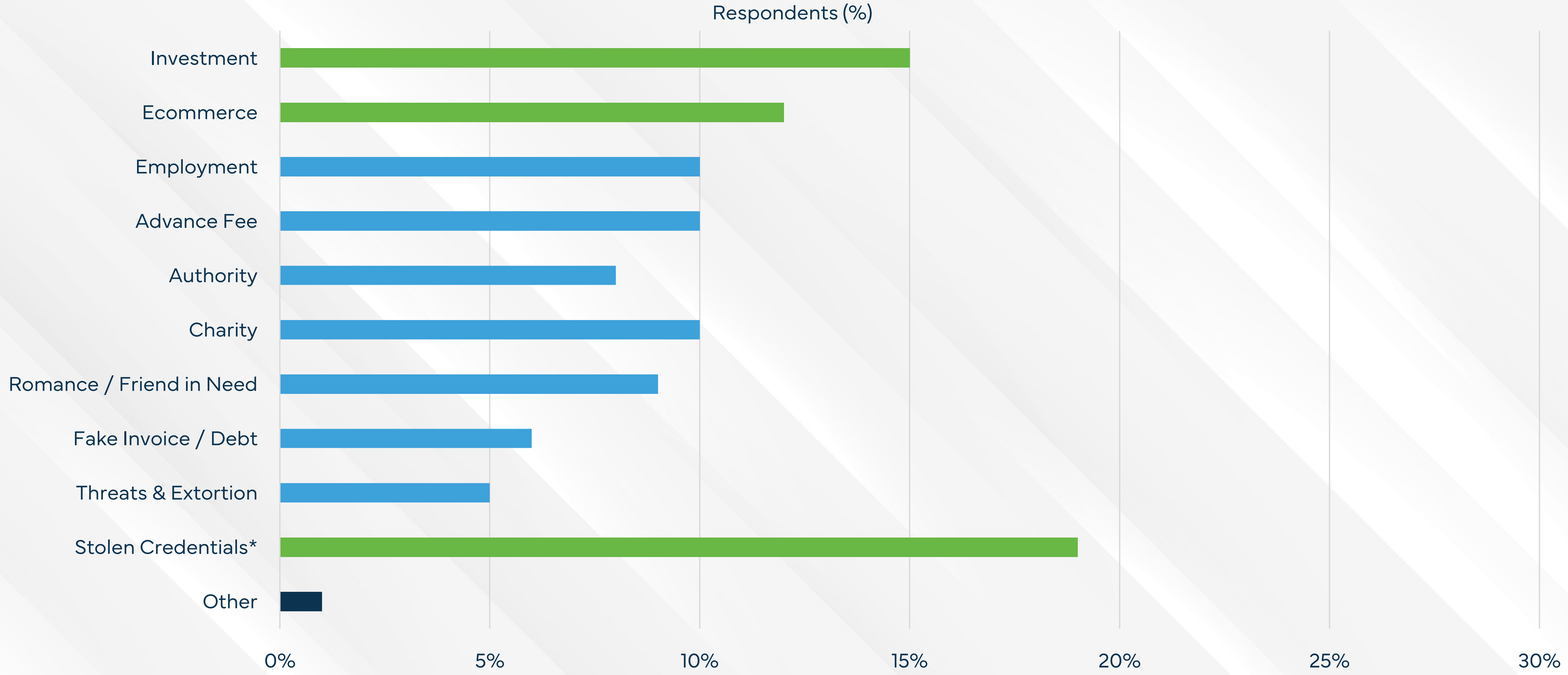
Most respondents think that AI was used to scam them



Only 14% did not think that the scam message they received was created by AI

Q9 - Do you think Artificial Intelligence (AI) was used in an attempt to scam you?

Respondents reported that many had their credentials stolen



Investment and ecommerce related types of scam experiences were also reported among the top three

Q10 - Which of the following negative experiences happened to you in the last 12 months?

*Stolen credentials refer to the use of personal information (e.g. bank, email or social media accounts) or credit card details without consent, to transfer money, take out a loan, request official documents or buy products/services, for the scammer's financial gain.

Singapore scam victims share their stories

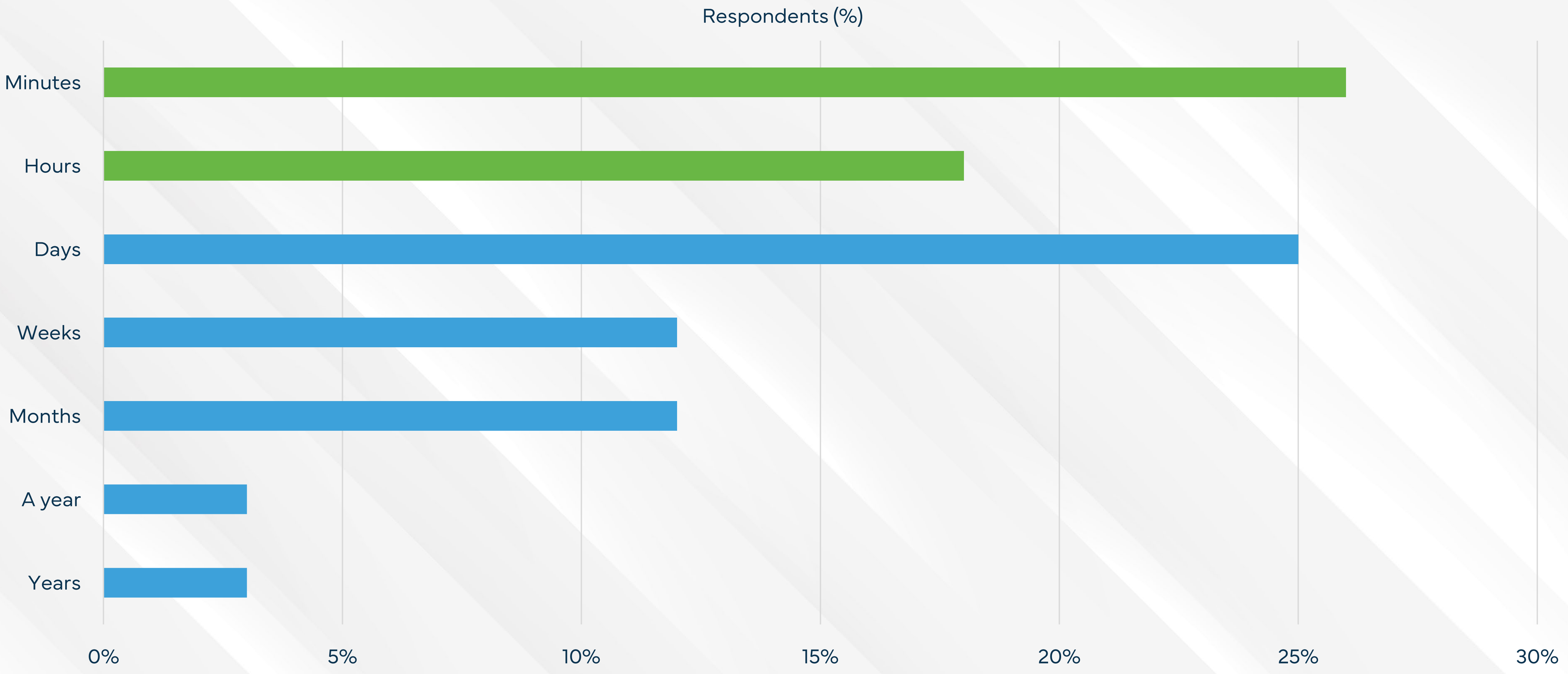
“I was misled into believing I was in a romantic relationship, but the scammer turned out to be manipulative and extortive, taking on multiple roles to extract money from me.”

“They offered you a part-time job where you could earn $300 per day. All you need to do is click on an advertisement, like the page, and like the post. After that, they invite you to join a Telegram chat group where you’re given tasks that require you to send money in advance, with promises of earning a 30% profit. The tasks involve three payments, with each payment amount increasing until you’re asked to pause and even borrow money from friends to make further payments, supposedly so you can receive your profits back in the end.”

“I received a WhatsApp message from an unknown number offering a job with an attractive salary. Thinking it was a legitimate offer, I replied and began a conversation with the person, who explained that the job involved completing orders and helping with SEO by clicking and submitting high ratings for various hotels. They also required me to set up a Bitcoin account for payment purposes. Fortunately, I sensed something was off and reported it to the scam hotline.”

“I received a call informing me that my bank account would be suspended and that I needed to follow instructions to transfer a payment.”

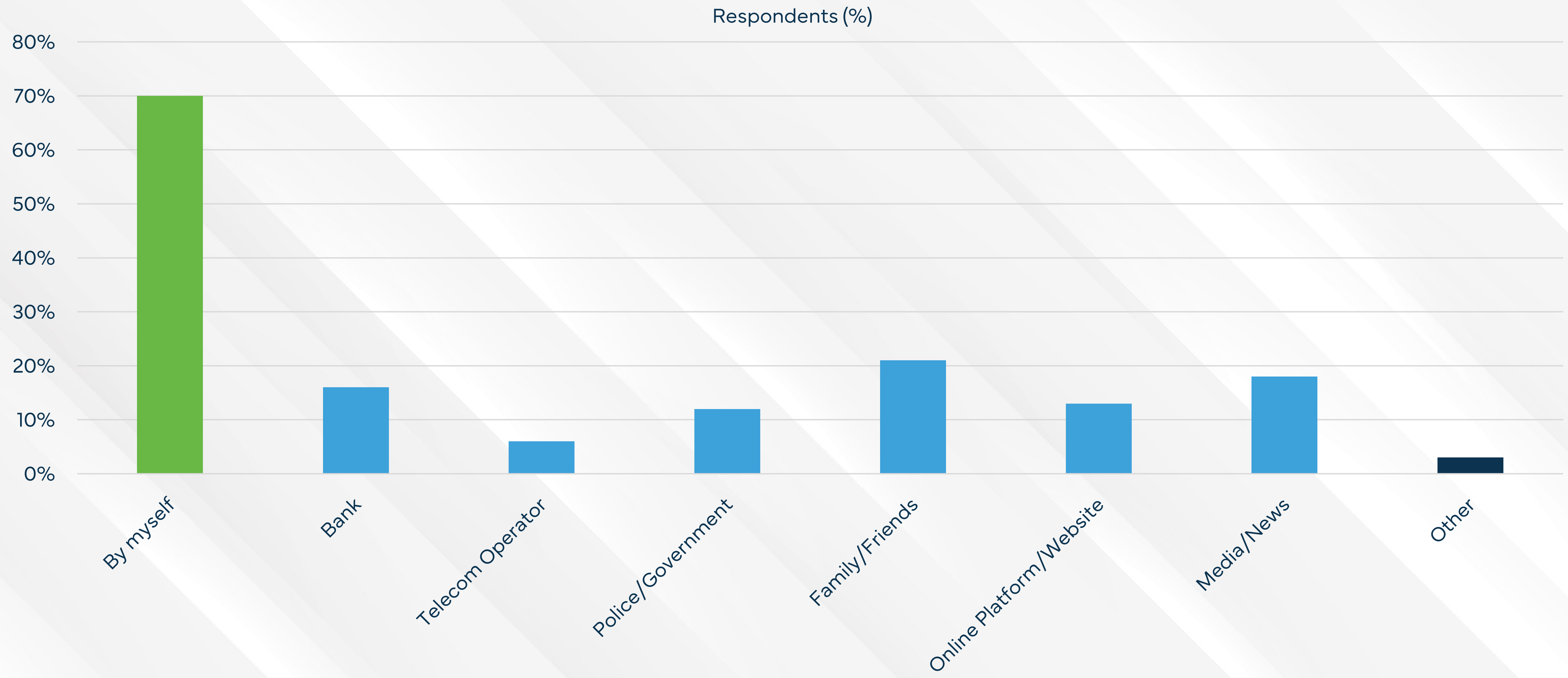
44% of scams were completed in less than a day



26% reported that the scam was over in a matter of minutes, while only 6% of scams took a year or more to complete

Q12 - How long did the scam last, from the first time you heard from the scammer until the last payment you made or the last time you contacted them?

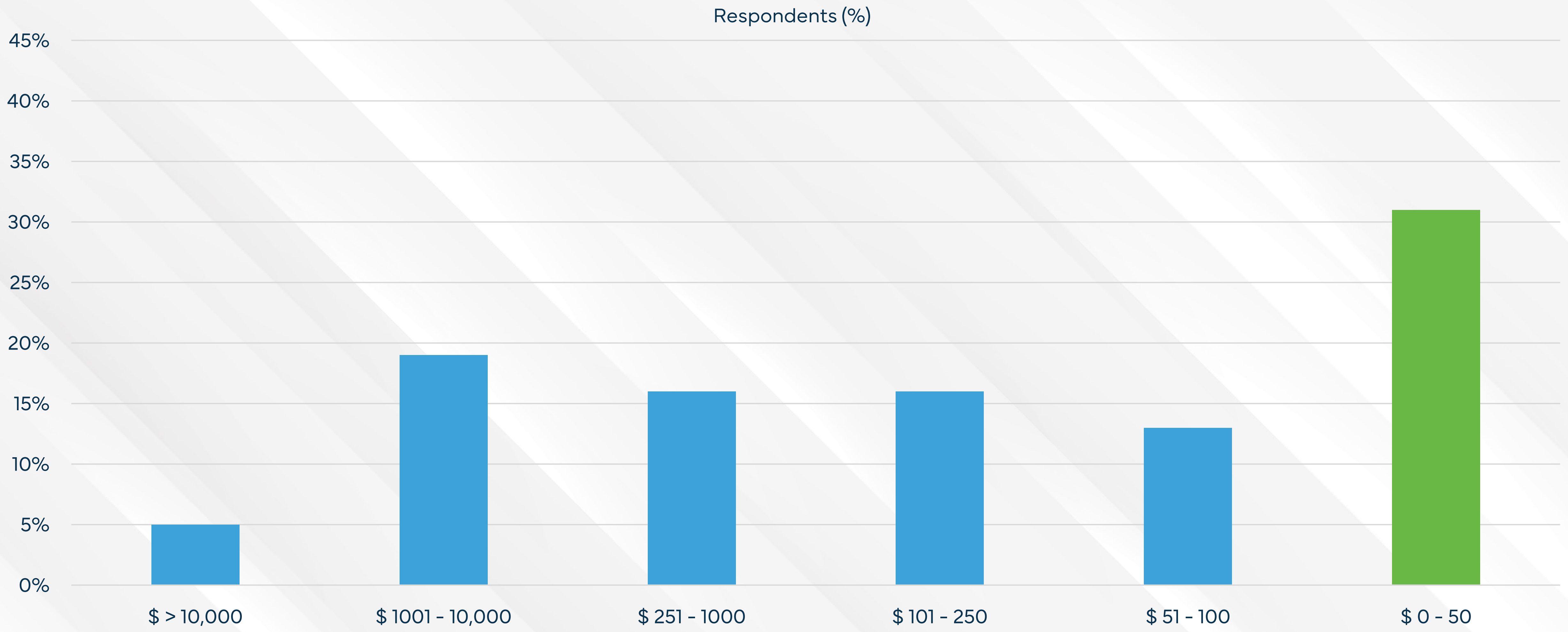
70% of respondents were able to reach their own realization that they have been scammed



Family/Friends and Media/News play an important role as well in informing victims about scams

Q13 - How did you discover you were scammed?

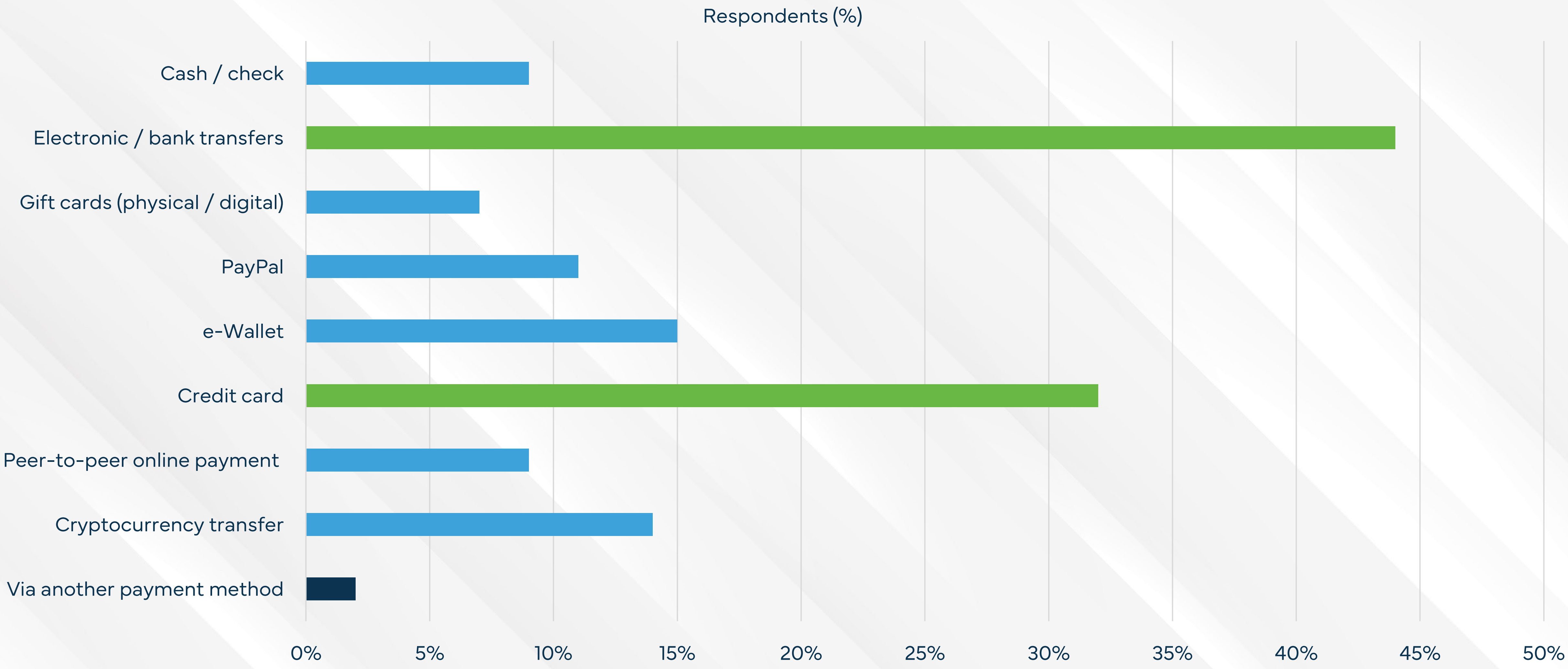
Most participants lost less than US$ 100 in the last 12 months



According to survey respondents, the average amount they lost in a scam was US$ 2,428

Q14 - In the last 12 months, in total, how much money did you lose to scams before trying to recover the funds?

Bank Transfer & Credit Cards were the top payment methods for scams

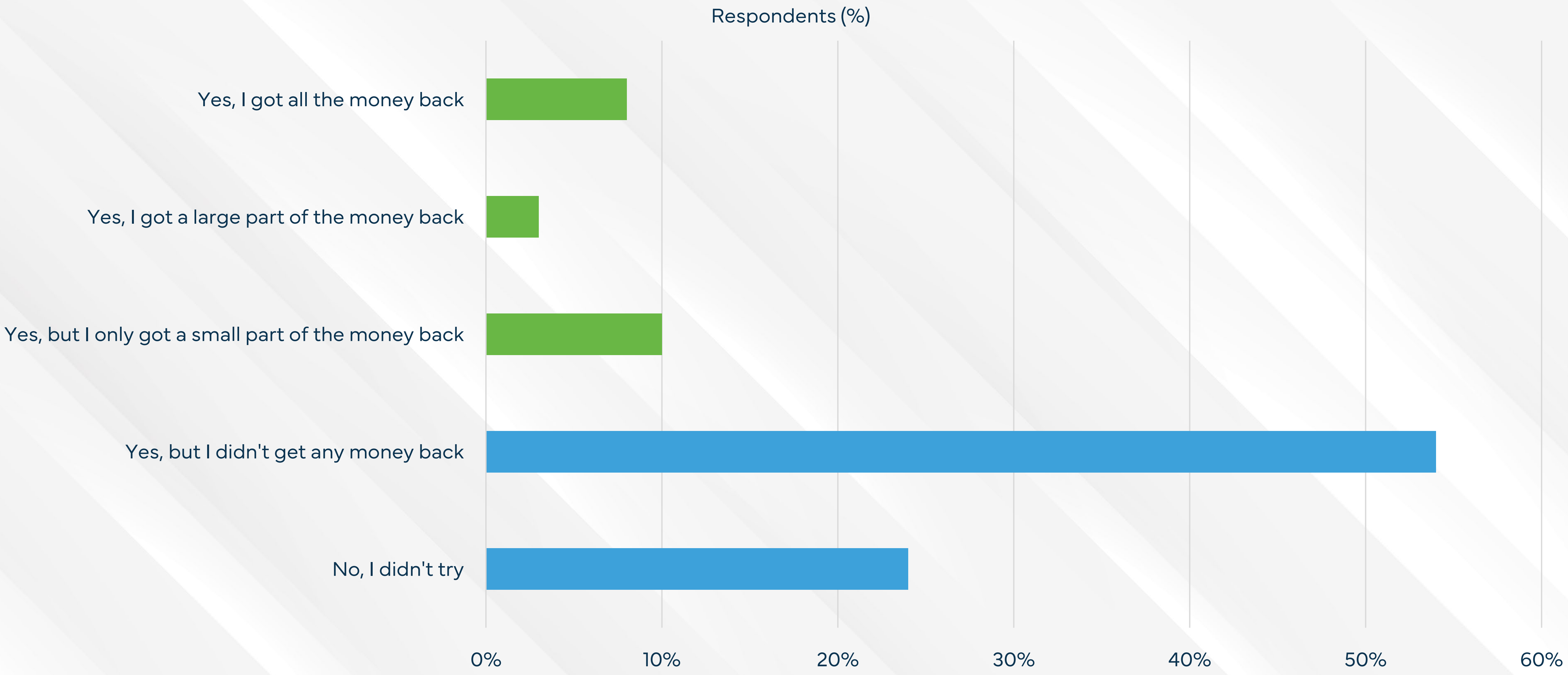


PayPal and e-wallet transfers were also popular payment methods to scammers.

Q15 - How did you pay the scammer?

Only 8% of victims claimed that they were able to recover their monies

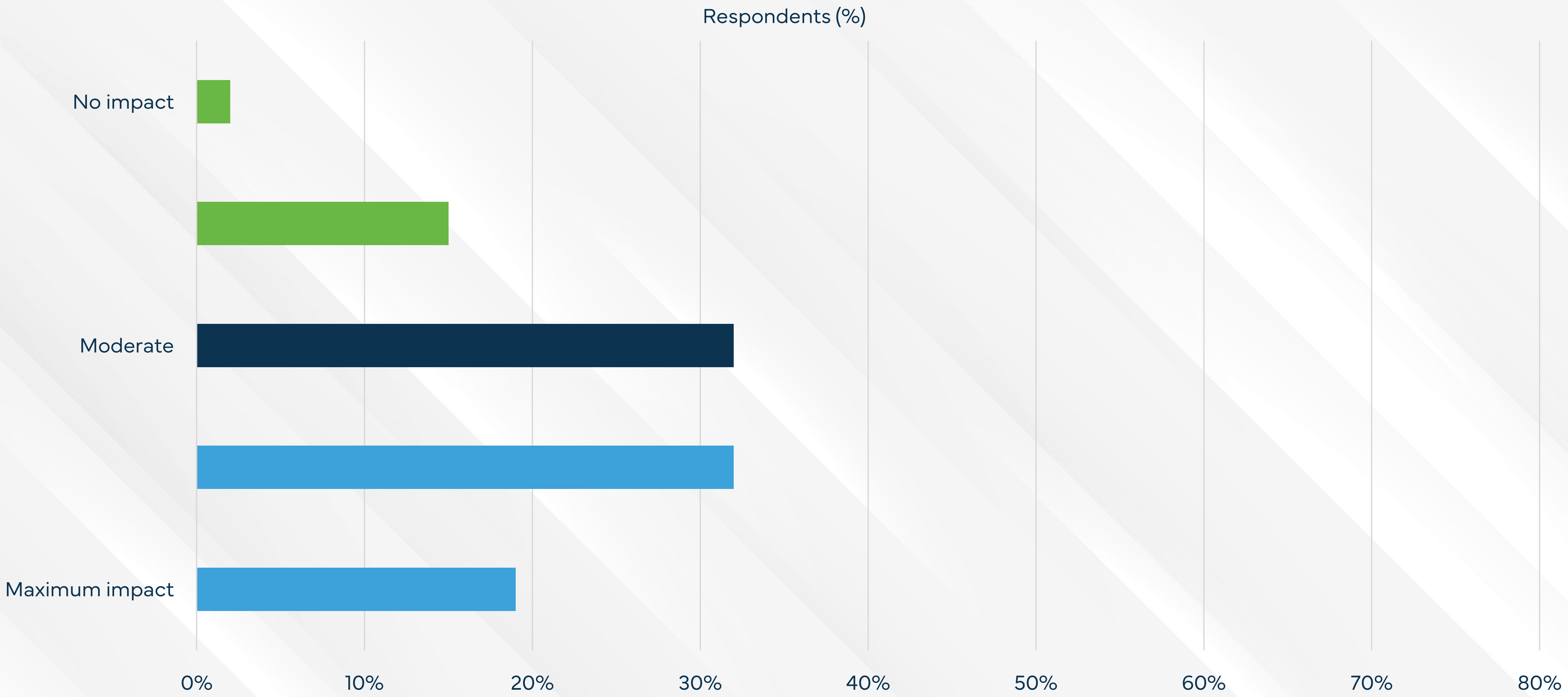
feedzai GASA Global Anti-Scam Alliance



54% say they tried but were not able to recover their monies.

Q16 - Did you try to recover the money lost?

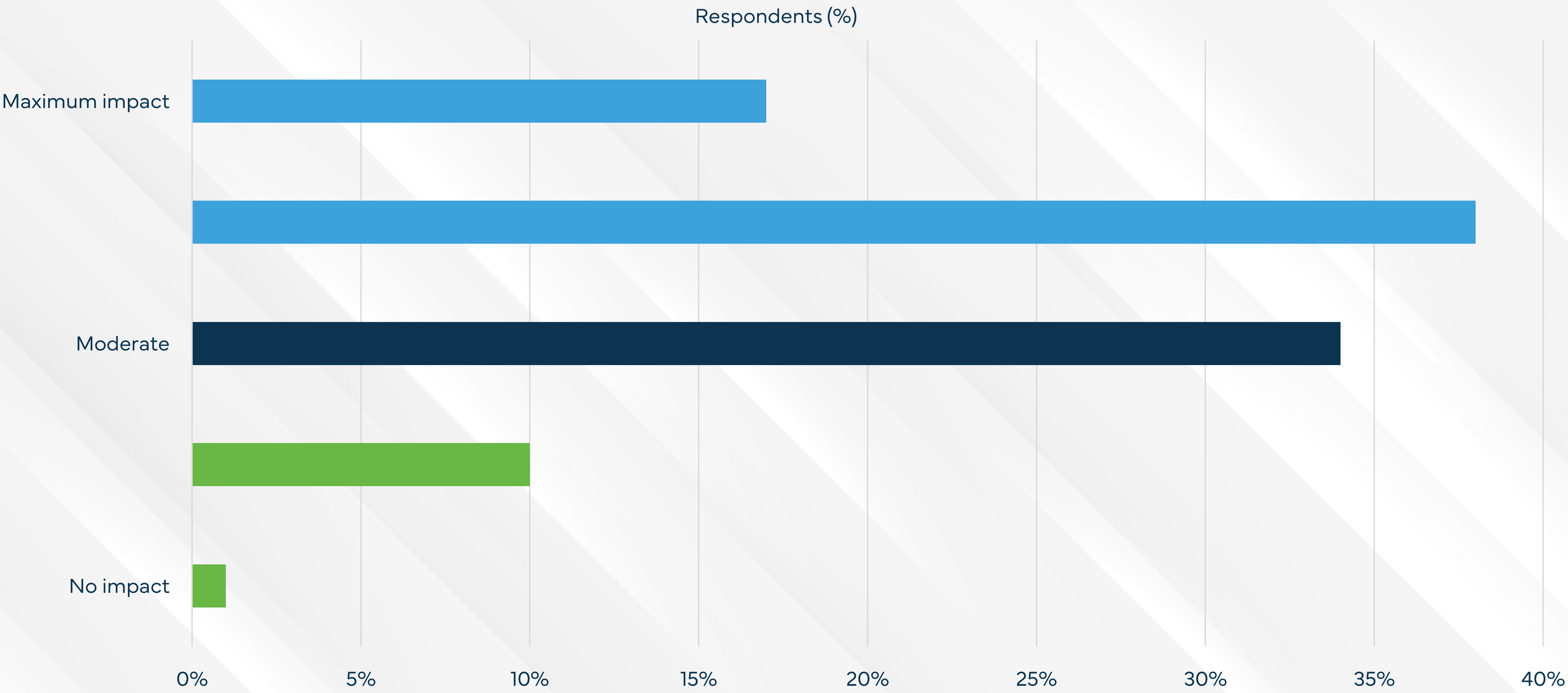
51% of victims reported moderate to significant emotional impact



17% of the survey respondents reported little to no emotional impact due to scams.

Q17 - To what extent did the scam(s) impact you emotionally?

55% of Singaporeans have lost trust in the Internet as a result of scams

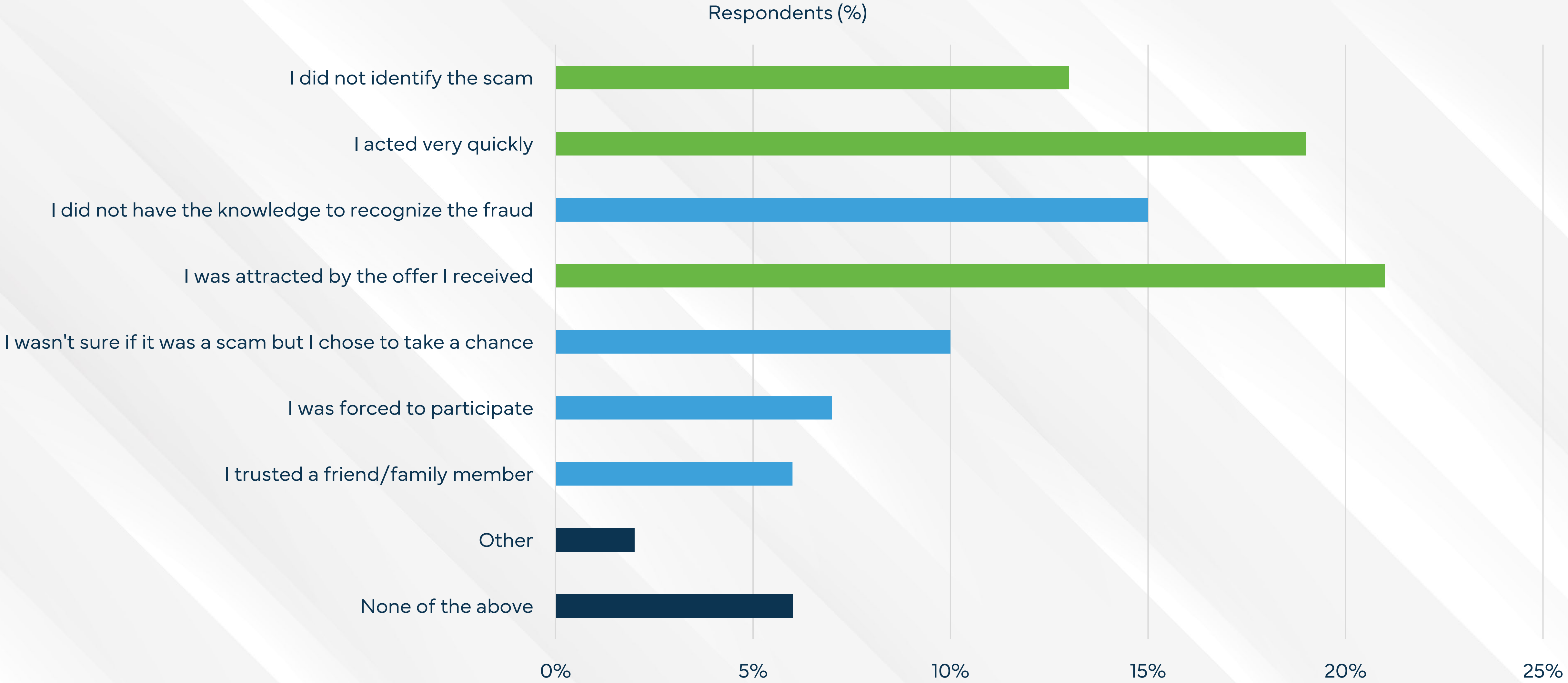


45% of the Singapore respondents reported little to no loss of trust in the Internet due to scams.

Q18 - To what extent do scams impact your trust in the Internet, in general?

About half of the victims fell prey to a scam because they were attracted by the offer, they acted too quickly, or they did not think it was a scam

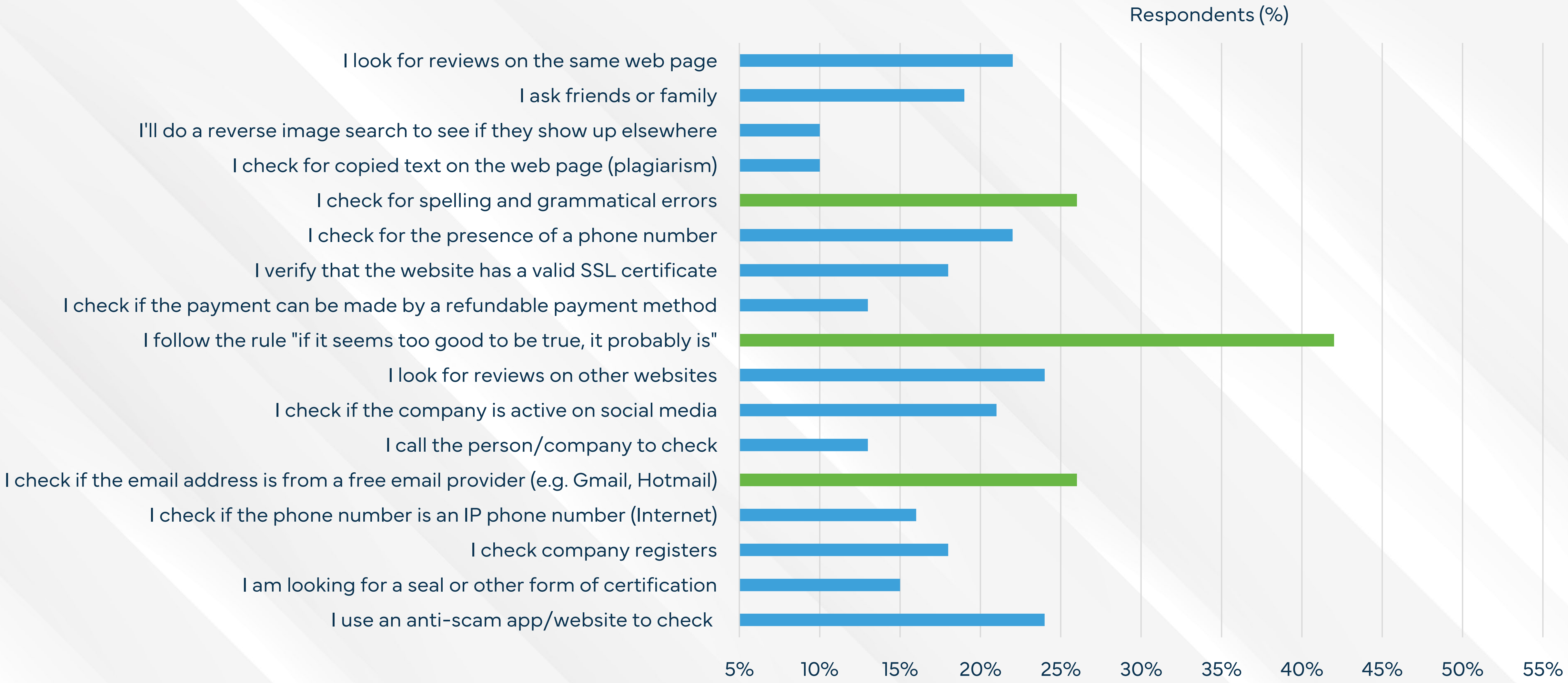
feedzai GASA Global Anti-Scam Alliance



Several victims were also unsure or did not have the knowledge to recognise scams.

Q19 - What was the main reason you were deceived?

Many respondents demonstrated some level of healthy skepticism and were able to pause and check

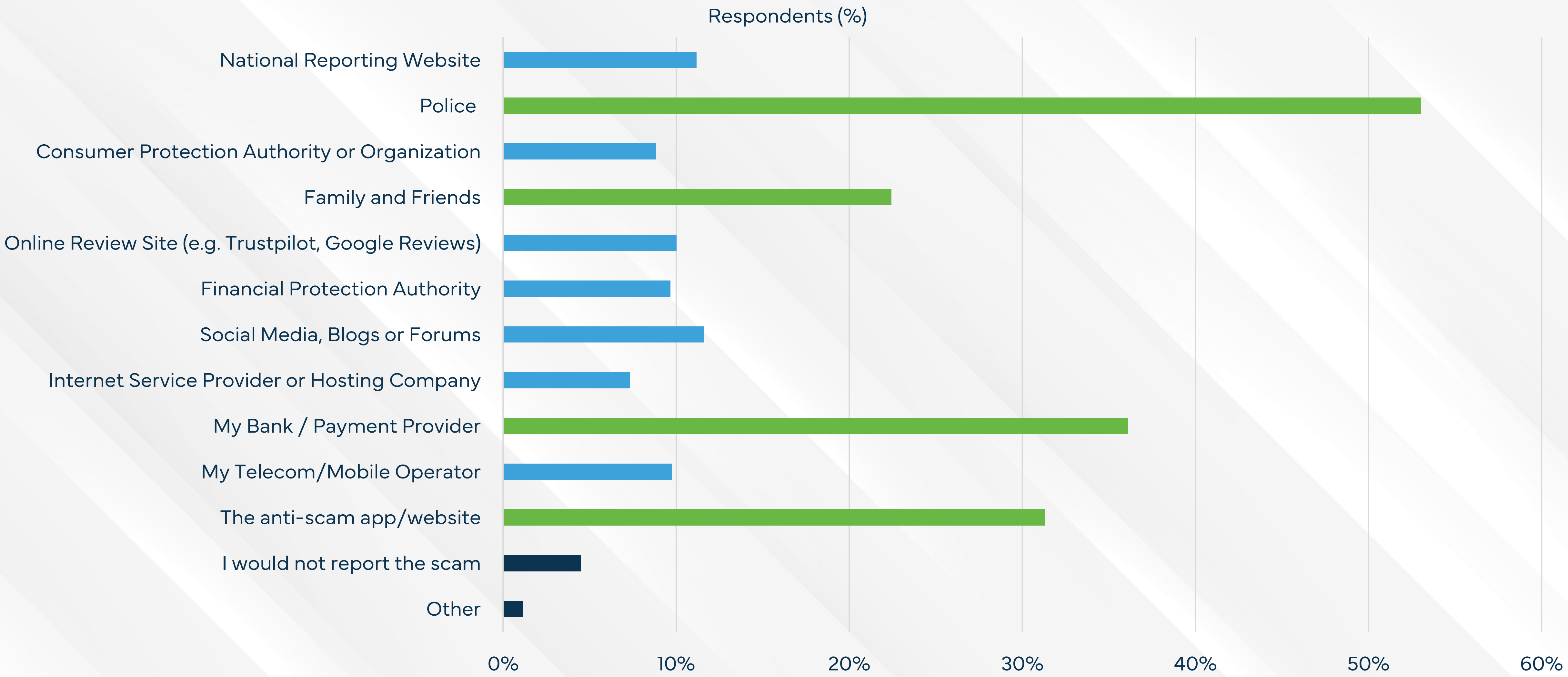


A number of respondents could detect other inconsistencies, such as spelling and grammar errors or email addresses.

Q20 - What steps do you take to check if an offer is real or a scam?

More than 50% of respondents would opt to report scams to the police

feedzai GASA Global Anti-Scam Alliance



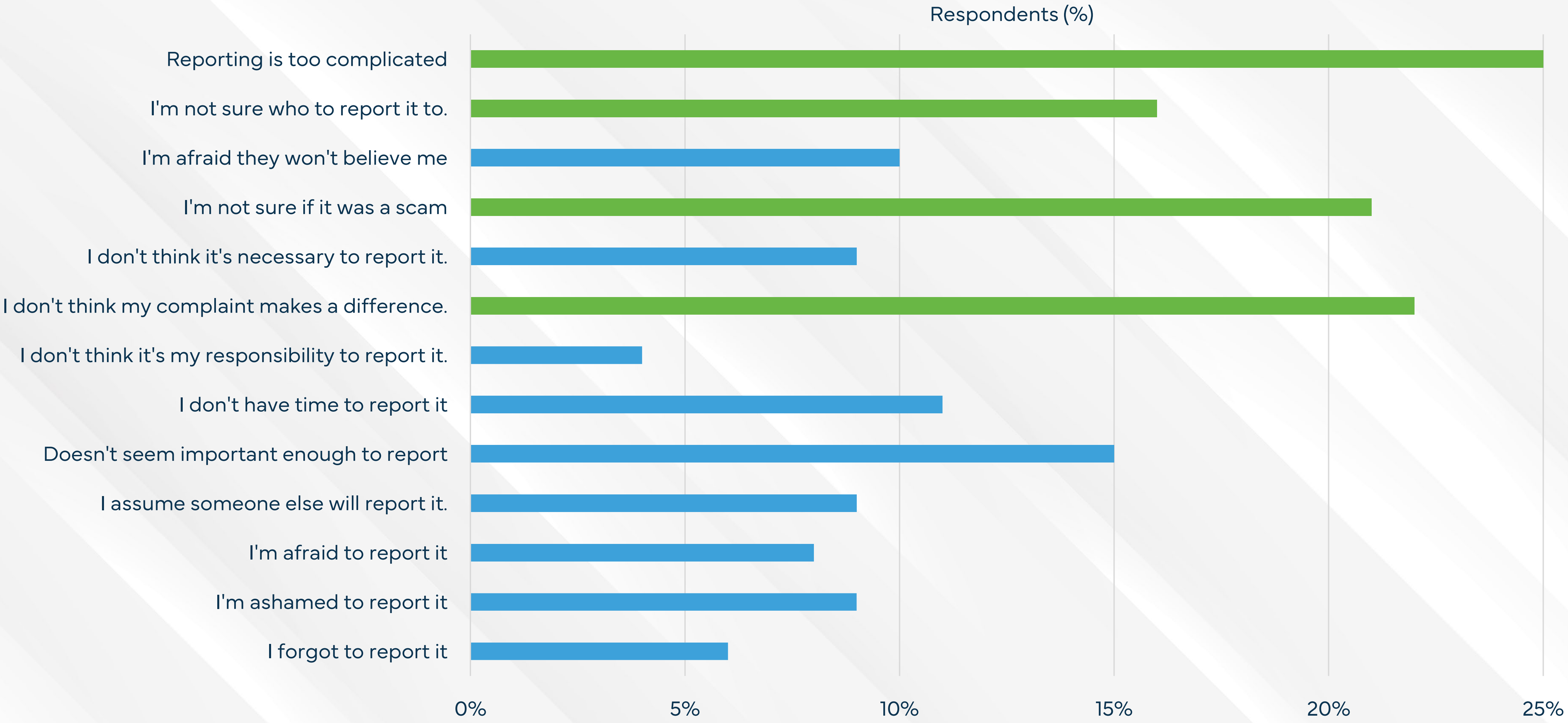
Anti-scam app/websites, National Police Agency and family/friends are also common places to report scams.

Q21 - If you were to be deceived by a scam, who would you report this to?

Many respondents found the process of reporting a scam too complicated

feedzai

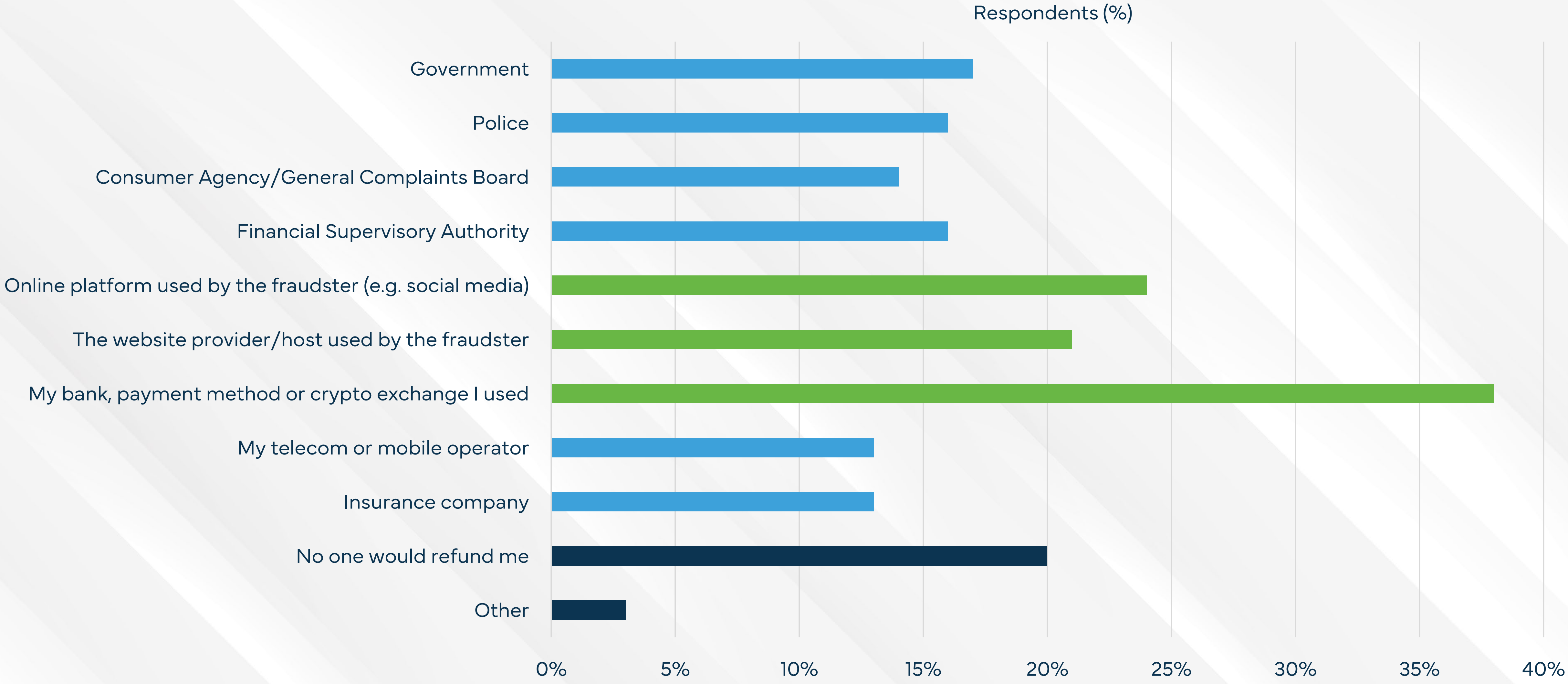
GASA Global Anti-Scam Alliance



Other respondents were unsure or if reporting it would make much of a difference.

Q22 - What reasons might you have to not report a scam?

More than half of respondents believe that banks and online platforms/websites should be responsible for scam losses

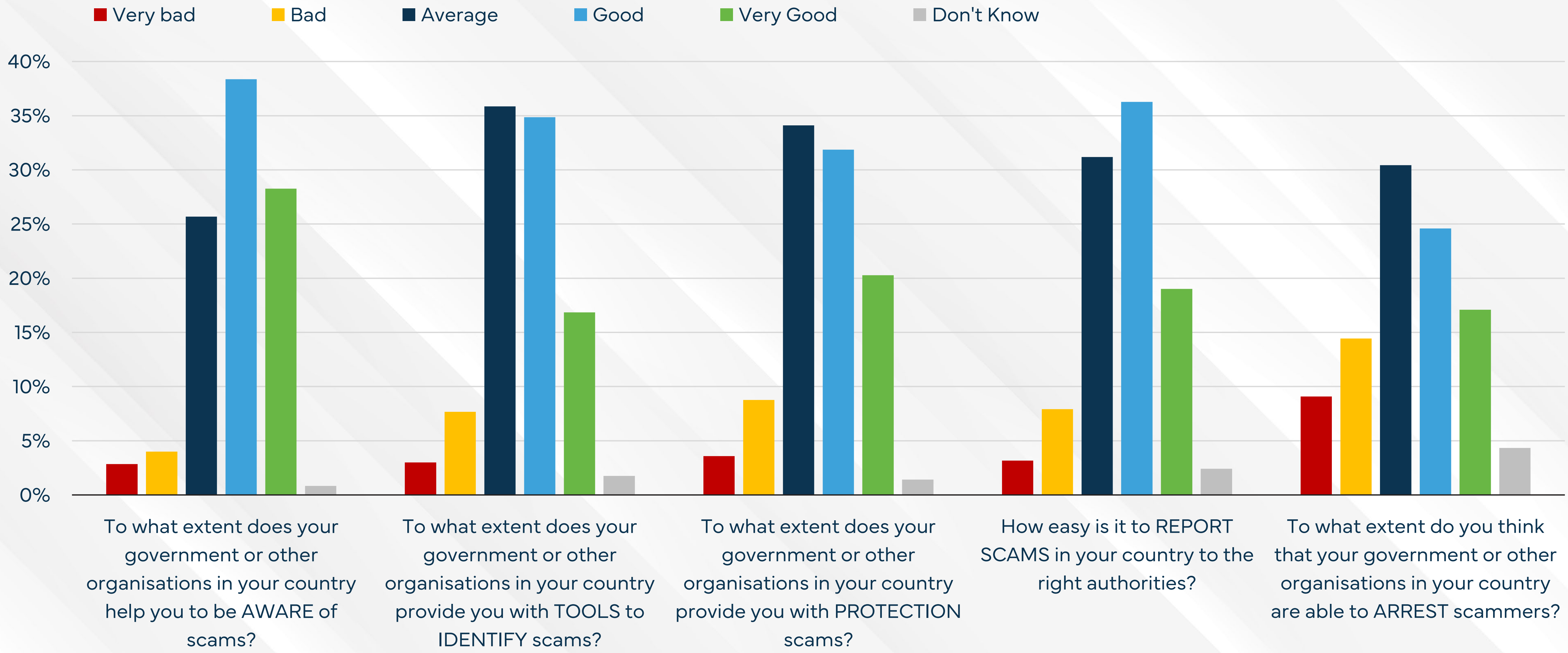


20% of respondents did not believe that they would receive any form of compensation.

Q23 - If you were scammed, who do you think should be responsible for making sure you are paid back for your loss?

Respondents were largely satisfied with the Government's anti-scam efforts

feedzai GASA Global Anti-Scam Alliance

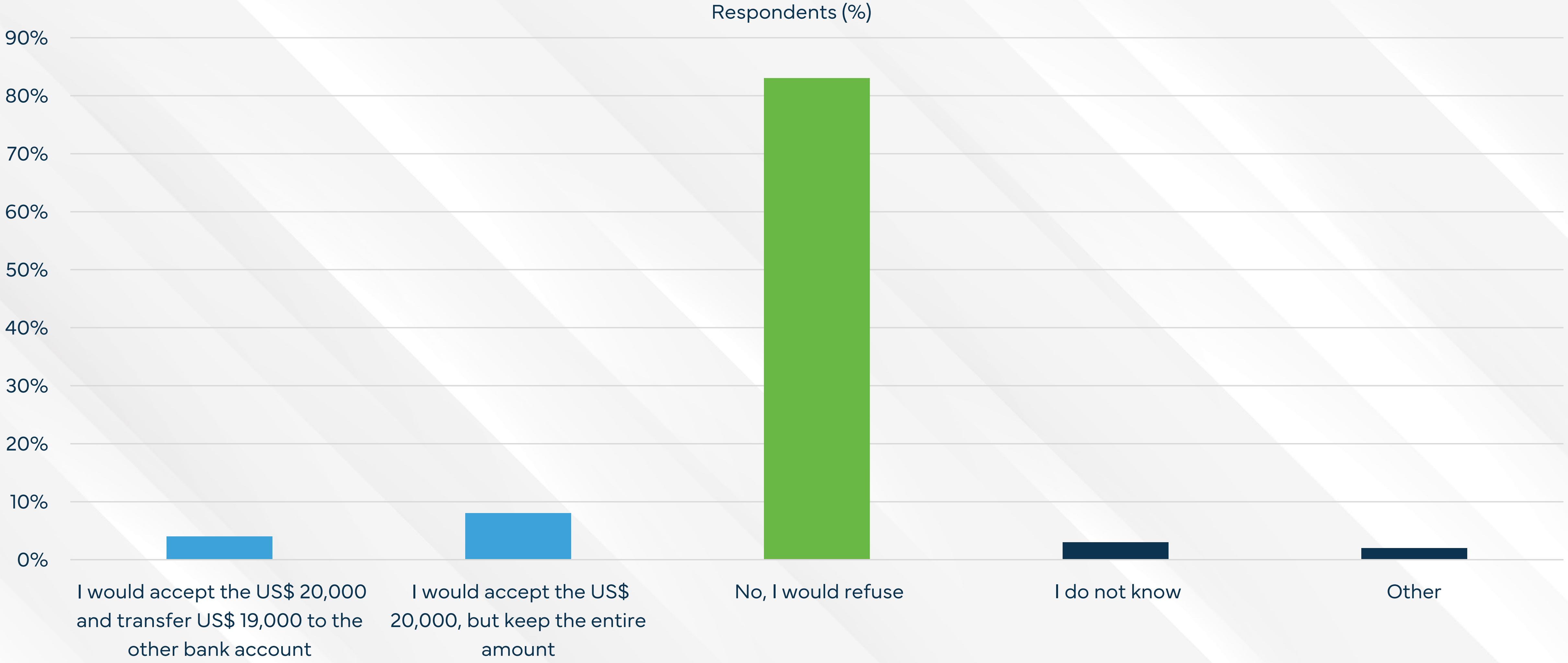


There was noticeably less confidence in the Government's ability to arrest scammers.

Q24 - Think about how well the government and other groups in your country are doing in the fight against online scams. How do you rate their efforts in the following categories?

More than 80% of respondents say that they will refuse to be involved in a money mule scam

feedzai GASA Global Anti-Scam Alliance



Less than 12% were attracted by the offer and was keen to participate.

Q25 - If someone offers you US$ 20,000 on the condition that you send US$ 19,000 to another bank account, leaving you with US$ 1,000 to keep, what would you do?

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. GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various countries.

Feedzai is the market leader in fighting financial crime with AI. We're coding the future of commerce with today's most advanced risk management platform powered by big data and machine learning. Feedzai built the world's first RiskOps platform specifically engineered and patented to combat financial crime. Our customers spend less time thinking about risk and more time growing their business.

Methodology

1. Survey Administration:

- **Tool Used:** Pollfish.com
- **Methodology:** Random Device Engagement (RDE), a successor to Random Digit Dialing (RDD), delivers surveys through popular mobile apps to a neutral, unsuspecting audience. This approach minimizes premeditated survey-taking biases.

2. Incentives and Fraud Prevention:

- **Incentives:** Non-monetary perks, such as extra lives in games or access to premium content.
- **Fraud Prevention:** Advanced AI and machine learning technologies to remove biased responses and enhance data quality.

3. Data Correction and Estimation Challenges:

- **Statistical Corrections:** Adjustments made based on the general demographic distribution within each country to account for potential biases in age or education level.
- **Estimation Limitations:** Outliers were removed as needed, and losses under one bitcoin were not included due to reporting constraints.
- **Estimated Amount Lost:** To calculate the total amount lost per country, we followed these steps:
  - Percentage of Participants Losing Money: We first determined the total number of participants who reported losing money in each country. This number was then divided by the total number of survey participants from that country to get the percentage of people who lost money.
  - Estimating the Total Number of Scam Victims: We multiplied the percentage of participants who lost money by the total population over 18 years old in that country. This gave us an estimate of the total number of scam victims in each country.
  - Calculating the Average Amount Lost: The average amount lost per person was calculated by averaging the reported losses from participants in each country, after removing any outliers that could skew the results.
  - Total Money Lost: Finally, we multiplied the estimated total number of scam victims over 18 years old by the average amount lost in their respective country. This provided the estimated total financial loss due to scams for each country.
  - This methodology ensures that the data reflects a reliable estimate of the financial impact of scams across different populations and regions.
- **Survey Respondents by Country:** The data presented in this report has been carefully weighted to account for differences in population size across the countries surveyed. This ensures that the findings accurately reflect the relative prevalence of scams in each country, irrespective of the total number of respondents. The weighting process allows for a more balanced comparison between countries with varying population sizes.
- **The total number of individuals who completed the survey varies by country, with respondent numbers as follows**: Argentina: 1,000 | Australia: 1,000 | Austria: 500 | Belgium: 880 | Brazil: 1,322 | Canada: 1,360 | China: 1,000 | Denmark: 556 | Egypt: 1,000 | France: 2,000 | Germany: 2,000 | Hong Kong: 511 | India: 1,000 | Indonesia: 1,000 | Ireland: 1,000 | Italy: 1,000 | Japan: 921 | Kenya: 1,000 | Malaysia: 1,202 | Mexico: 1,000 | Netherlands: 1,012 | New Zealand: 1,071 | Nigeria: 1,000 | Pakistan: 1,000 | Philippines: 1,000 | Poland: 1,000 | Portugal: 1,000 | Romania: 1,000 | Russian Federation: 1,000 | Saudi Arabia: 500 | Singapore: 1,199 | South Africa: 1,000 | South Korea: 708 | Spain: 1,000 | Sweden: 574 | Switzerland: 269 | Taiwan: 5,003 | Thailand: 9,630 | Türkiye: 1,000 | United Arab Emirates: 1,964 | United Kingdom: 2,000 | United States: 2,500 | Vietnam: 647.

Of the 94,954 people approached with the Global State of Scams 2024 survey, fully completed surveys were submitted by 58,329 individuals across 42 countries.

4. Additional Data Sources:

- **Inhabitants per country:** Worldometers.info
- **Currency conversion:** Xe.com
- **Internet penetration:** Wikipedia
- **GDP Estimate 2024:** Wikipedia

5. Translation and Localization:

- **Procedure:** Each survey was translated and localized by a human to align with the official or most commonly spoken language of the target country.

6. Inspirational Reference:

- **Study:** The methodology was partly inspired by the findings of DeLiema, M., Mottola, G. R., & Deevy, M. (2017) in their pilot study to measure financial fraud in the United States (SSRN 2914560).

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 & European Ecommerce Association) and the Ecommerce Foundation.

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

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 GASA's Director of Marketing. Previously, he worked in Risk Advisory, before transitioning into a career as a researcher, copywriter, and content manager specialized in cutting-edge electrical engineering topics, such as photonics and the industrial applications of electromagnetic radiation.

Sam left the world of corporate industry seeking a role which would allow him to concentrate on networking and events management, while allowing him to contribute something worthwhile to society.

James Greening, operating under a pseudonym, brings a wealth of experience to his role as a scam investigator, content writer, and social media manager. Formerly the sole driving force behind Fake Website Buster, James leverages his expertise to raise awareness about online scams. He currently serves as a Content Writer and Social Media Manager for the Global Anti-Scam Alliance (GASA) and regularly contributes to ScamAdviser.com.

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

Join the Network to Beat a Network

feedzai

GASA
Global Anti-Scam Alliance

INTELLIGENCE SHARING

Regular Virtual Meet-ups
8 Topic-based Email Groups
10,000 Professionals Newsletter

RESEARCH

Global State of Scams
30+ Regional Reports
Policy Papers

NETWORKING

3 International Summits
Online Member Directory
National GASA Chapters

CYBERCRIME EXCHANGE

80+ Pooled Data Sources
Realtime Data Sharing
Access to Global Leaderboards

OUR FOUNDATION PARTNERS

amazon

Bitdefender

Capital One

feedzai

Gogolook

Google

SCAMADVISER

Meta

TREND MICRO

Match Group

Become a member, see all member benefits at: gasa.org/membership

feedzai

Disclaimer

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

Global Anti-Scam Alliance (GASA)
Oder 20 - UNIT A6311
2491 DC The Hague
The Netherlands

Email: partner@gasa.org
X (Twitter): @ScamAlliance
LinkedIn: linkedin.com/company/global-anti-scam-alliance

GASA
Global Anti-Scam Alliance