BioCatch

The State of Scams in Sweden 2024

GASA
Global Anti-Scam Alliance

Fraudsters target 1-in-8 as Swedes lose $2.75 billion in 12 months

Welcome to the **2024 State of Scams in Sweden** report, a study carried out by the Global Anti-Scam Alliance (GASA) and BioCatch. Our research has revealed that the Swedish people are having to contend with a rapidly evolving series of digital threats, which manifest daily as trends shift from traditional fraudulent activities. As new AI-powered deceptions offer cybercriminals new ways to mask their identities & disguise their true intentions, our research seeks new insights in the digital sphere of scams.

There was a 17% drop in confidence in recognizing scams, with **13% encountering fewer scams** than in the previous year, compared to the 12% reported in 2023. However, a worrying **39% experienced an increase in scam attempts** in both 2022 & 2023, which contributes a **93% jump in annual scam encounters** over the 2 years!

The mediums for scams have shifted slightly, with emails and text messages remaining common channels. However, phone calls and social media scams have seen a slight increase, underscoring the adaptability and reach of scammers. In terms of reporting scams, the situation appears to have worsened in 2024, with an overwhelming **80% choosing not to report scams**, an increase from the 61% non-reporting rate in 2023. This highlights a growing reluctance or resignation among scam encounters. Speaking of mediums & tools, artificial intelligence (AI) quickly became the buzzword of the year, in 2023, which made it clear that we needed to include it in 2024.

While the emergence of AI will assist scammers in many cases, a significant portion of participants in 2024 acknowledged the role of AI in creating sophisticated fake texts, chats, voices, and images. Perhaps, we can thank the wide media coverage of AI evolution for its contribution to the awareness and education of consumers about this new threat.

In a comparative analysis of the 2023–2024 financial data on scams in Sweden, we observe the percentage of those financially impacted by scams held steady at 12%. A concerning trend is the uptick in the average amount lost to scams, escalating from $2,557 (26,609 Swedish Kronor) to **$2,726 (28,370 SEK)** per victim. This increase suggests that the financial severity has intensified over the past year.

The actual number of individuals over 18 affected by scams showed a slight decrease from 1,034,736 to **1,007,912**, a silver lining indicating a marginal downturn in victimization. However, the total financial loss due to scams rose, with an increase from approximately $2.646 billion (27.5 billion SEK) in 2023 to **$2.748 billion (28.6 billion SEK)** in 2024. As a result, fraudulent profit from **scams rose from 0.40% of Sweden's GDP to 0.50%**. It is worth reiterating, however, that these figures are estimates that take into account only 20% of Swedes report that they were scammed to anyone at all.

Sweden is facing a persistent threat from scams and the escalation of financial detriment per incident has worsened. There is a critical need for strategic countermeasures to combat the evolving tactics of fraudsters, reflecting an ever-present and complex challenge to both individuals & the Swedish economy.

The emotional impact of scams has intensified, with **57% of victims in 2024 reporting a strong emotional response**, up from 45% in 2023. This suggests that scams are becoming more personal and distressing for victims. Government efforts in combating online scams have a divided opinion in 2024, with **40%** considering them very good, contrasting sharply with the 45% who viewed them as very bad in 2023. This may suggest some improvements in government action or public perception.

This year, we included a hypothetical question about participating in a money mule scam, as we hope to shed light on the susceptibility of the public to such schemes. With **4%** of Swedes *admitting* that they would entertain the idea, it emphasizes the necessity for ongoing education and awareness campaigns.

Overall, while there are glimmers of improvement with fewer scams reported by some, the increased emotional toll, the significant percentage of people not reporting scams, and the advent of AI in scam creation underscore an urgent need for enhanced awareness, better reporting mechanisms, and a concerted effort to tackle this digital menace.

Jorij Abraham
Managing Director
Global Anti-Scam Alliance

Sweden needs "more proactive steps" to protect online consumers

BioCatch, a pioneering firm at the forefront of behavioral biometrics intelligence and advanced cyber solutions, brings an innovative approach to detecting and preventing digital fraud through user behaviour analysis has set new standards in the industry. In this interview, GASA speaks to Gareth Williams, a seasoned Pre-Sales Consultant at BioCatch, sheds light on the current state of scams in Sweden, the innovative tactics employed by fraudsters, and the unified efforts needed to safeguard consumers.

How big has the problem of scams become in Sweden? Like many countries in Europe, scams are increasing year-on-year. According to the Swedish Crime Prevention agency BRÅ, social engineering fraud increased by 36% during 2023, with around 650 cases of fraud reported daily. The Swedish Police report that over 660 million kronor were lost to fraud in 2023 – with half of those losses directly linked to social engineering. Yet GASA finds only 20% of Swedes report the scams committed against them. Sweden is often seen as a country well ahead of the digital curve and is a virtually cashless society. As a result, we are seeing criminals switch tactics – They are targeting individual consumers at an alarming pace, whilst for example there have been no reported bank robberies for over 2 years.

Which were trending in Sweden over the past year? Scams using a combination of smishing and vishing, some specifically targeting the elderly have been in the spotlight recently. One contributing factor is the availability of data in Sweden, where information on people, their addresses, phone numbers, age, income etc is readily available for a small fee. A documentary highlighting the way criminal gangs exploit the elderly in this way was recently broadcast on national TV, which has once again put the state of scams in Sweden into the spotlight across national media. In general, we are seeing that scam messaging in email and SMS is becoming better and better, which indicates that criminals are turning towards modern technology, like ChatGPT, to help craft convincing messages – A language spoken by a relatively small number of people is no longer holding international fraudsters back.

Which actions have been taken by the Swedish government and other organizations to protect consumers from scams? Any best practices from which we can learn? As a direct result of the documentary, the Swedish Prime Minister met with the Swedish Banking Association, heads of the largest banks and the Police. During the meeting, the government instructed banks to take a greater level of responsibility to protect consumers from scams and warned that if the situation doesn't improve then they will introduce new laws to force banks to keep consumers safe. The government requested the banks to work on improving technical solutions to make scams less successful.

Until now, we saw that consumers overall are held liable where they fall victim to scams and we may see changes to this during 2024. Many are looking at the steps the UK banks took with their voluntary code – This would allow banks to effectively self-regulate whilst also demonstrating that more is being done to tackle scams, rather than being forced to comply with government legislation. PSD3, once in force, will likely lead to a change in the way scam reimbursement is treated, at least in some cases.

What action would you like to see taken that could give consumers the upper hand in the fight against scams? Until now, consumer information campaigns have been the popular method to try to fight against scams. Keeping consumers informed is very important, but shouldn't be the only line of defence. We need to see more proactive steps from banks investing in technology which can detect the signs that a customer is being tricked into making payments and make Sweden a harder target.

Others in the scam ecosystem also have an important part to play. We've recently seen some progress with telecoms providers making it harder to "spoof" phone numbers, but again there is more that can be done to stop scammers using SMS as an entry point for "safe account" scams. Social media platforms also need to contribute by removing investment scam advertisements and putting more focus on purchase scams by taking down ads for goods that don't exist.

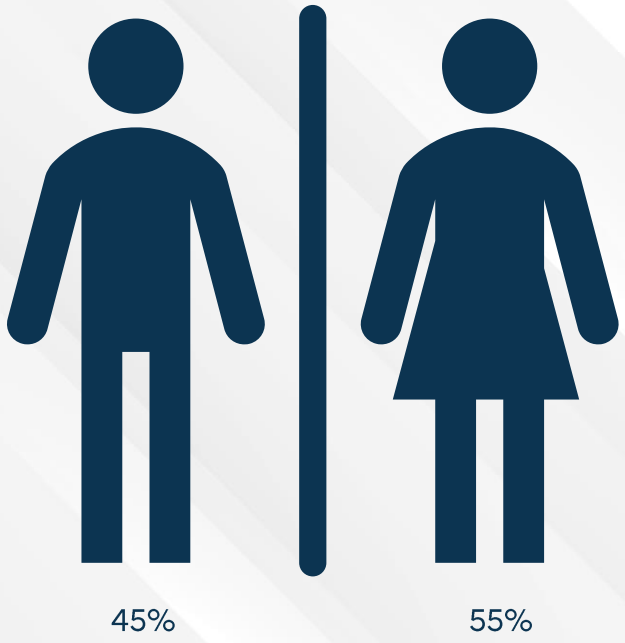
Gareth Williams
Pre-Sales Consultant
BioCatch

614 Swedes completed the State of Scams in Sweden survey

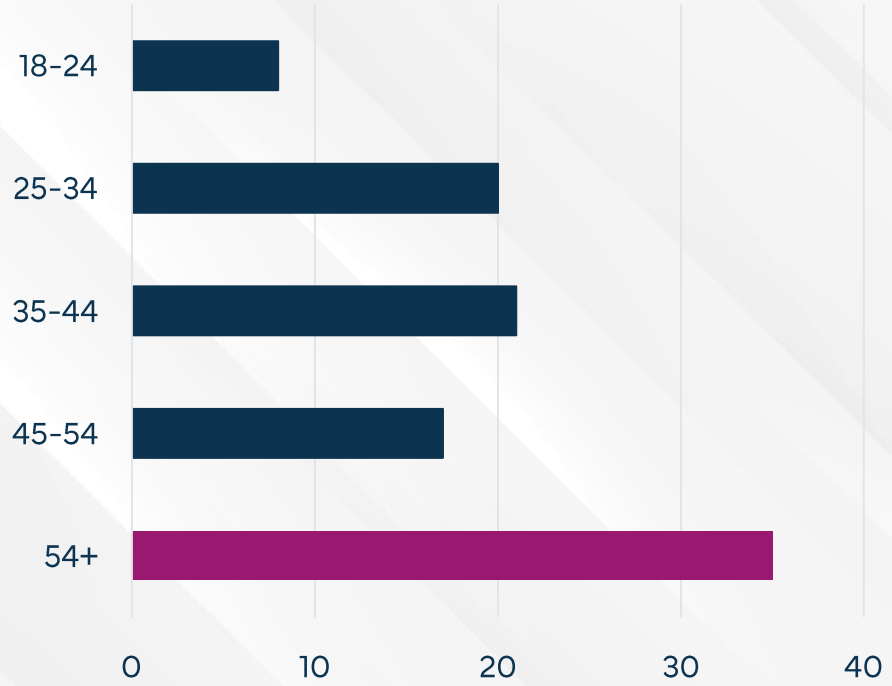
BioCatch

GASA
Global Anti-Scam Alliance

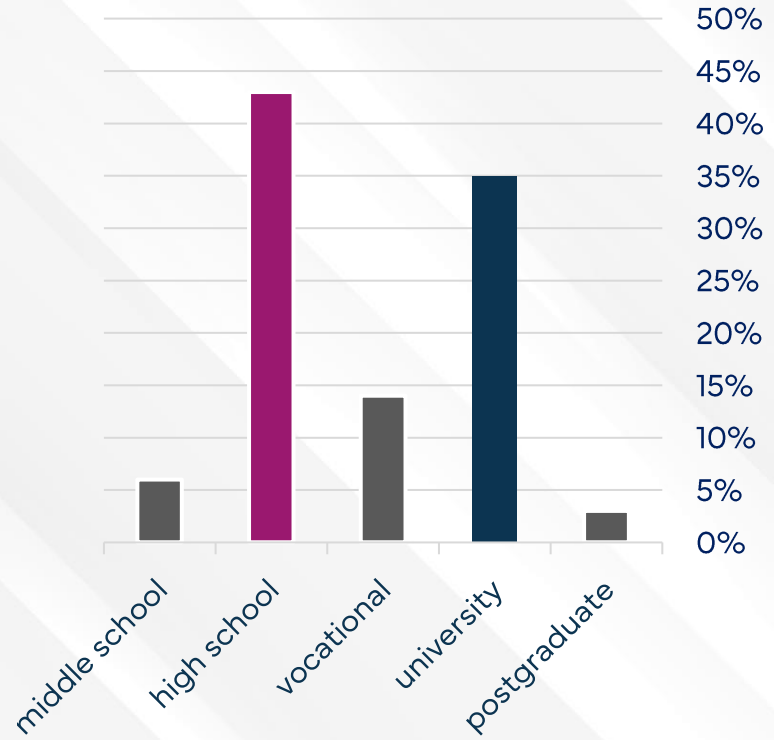
Gender



Age Range

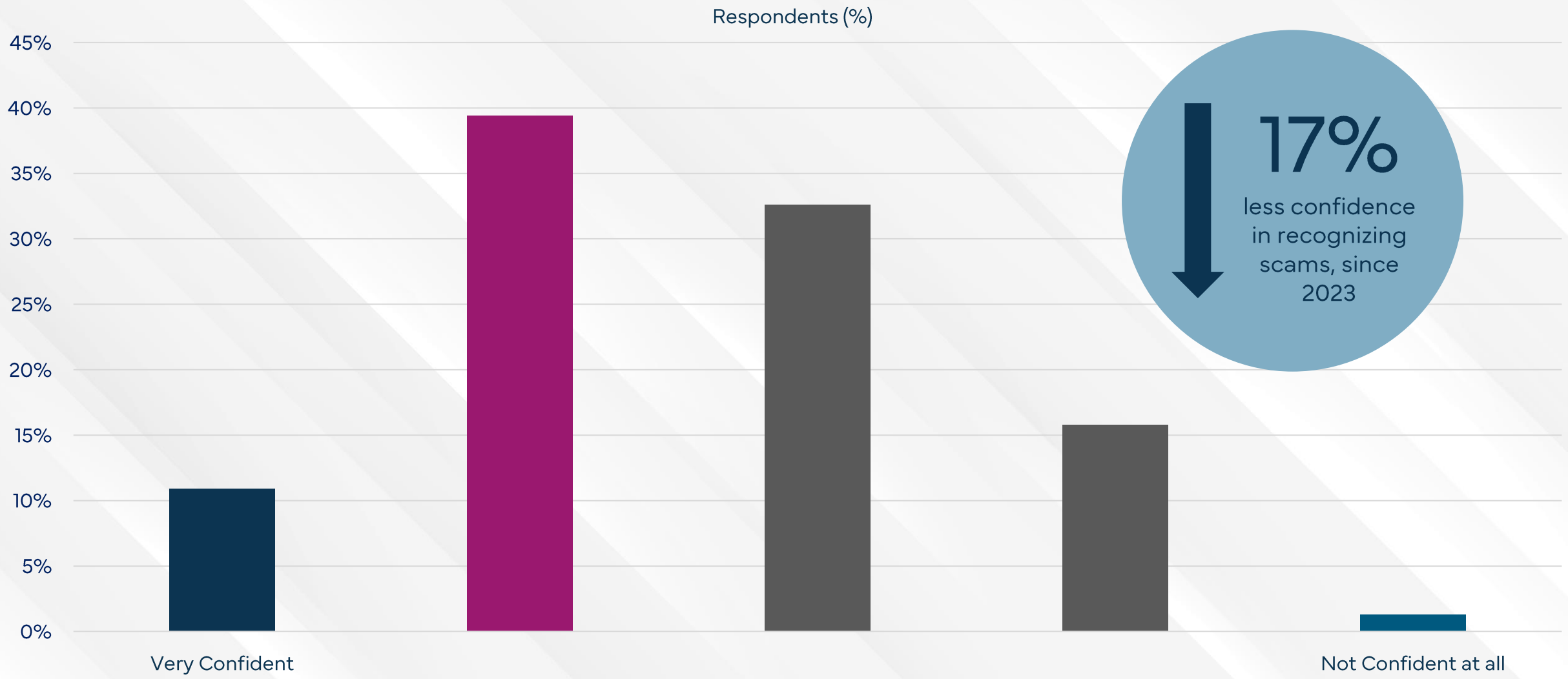


Education



The demography of respondents to the State of Scams in Sweden 2024 survey consists of slightly more women than men. A large proportion were over 54 years of age, with a high school education.

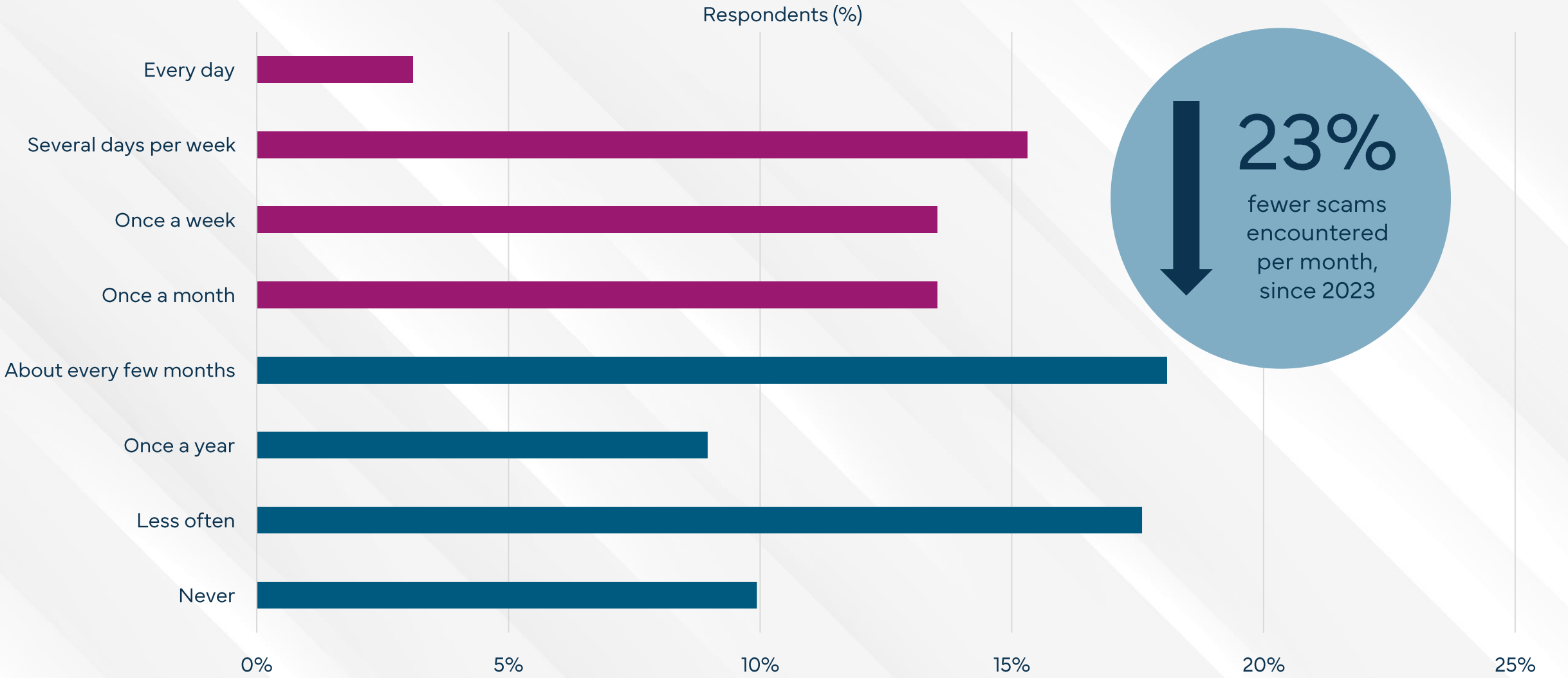
50% of Swedes are (very) confident of recognizing scams



Only 1% of respondents are not (very) confident in recognizing scams, at all.

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

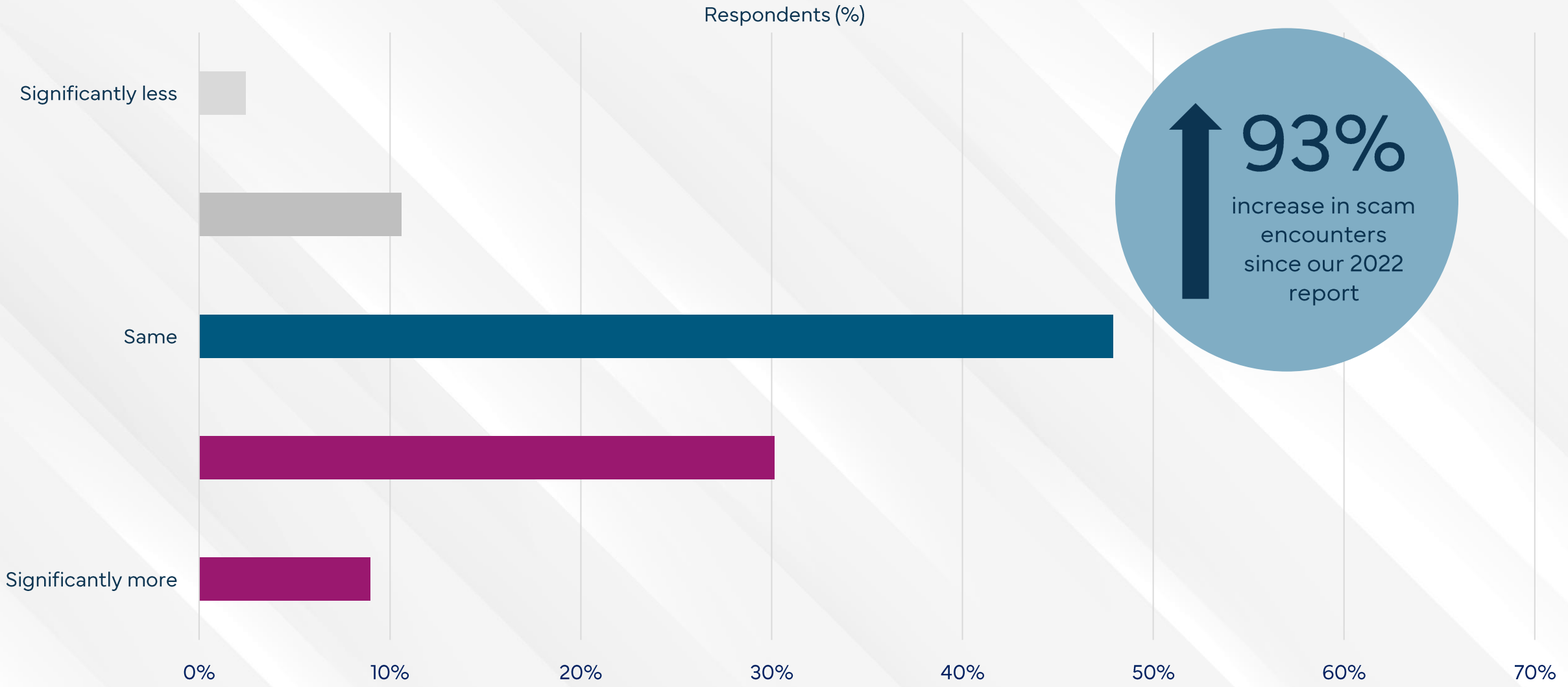
45% of Swedes encounter scams at least once per month



17.6% of Swedish respondents encountered fewer scams this year, compared to the previous 12 months.

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.

39% of Swedes had more scam encounters in the last 12 months

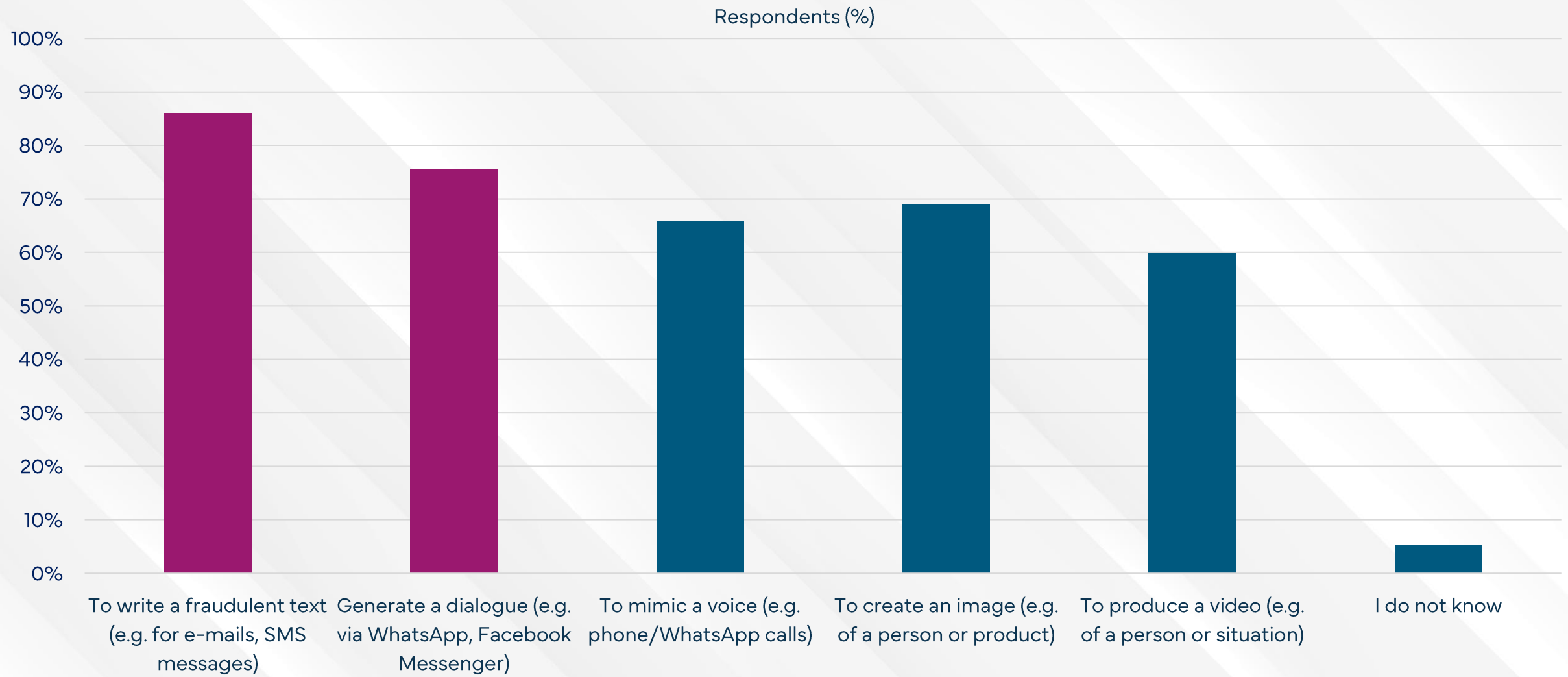


93%
increase in scam encounters since our 2022 report

Only 13% of Swedish respondents experienced a reduction in scam encounters.

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?

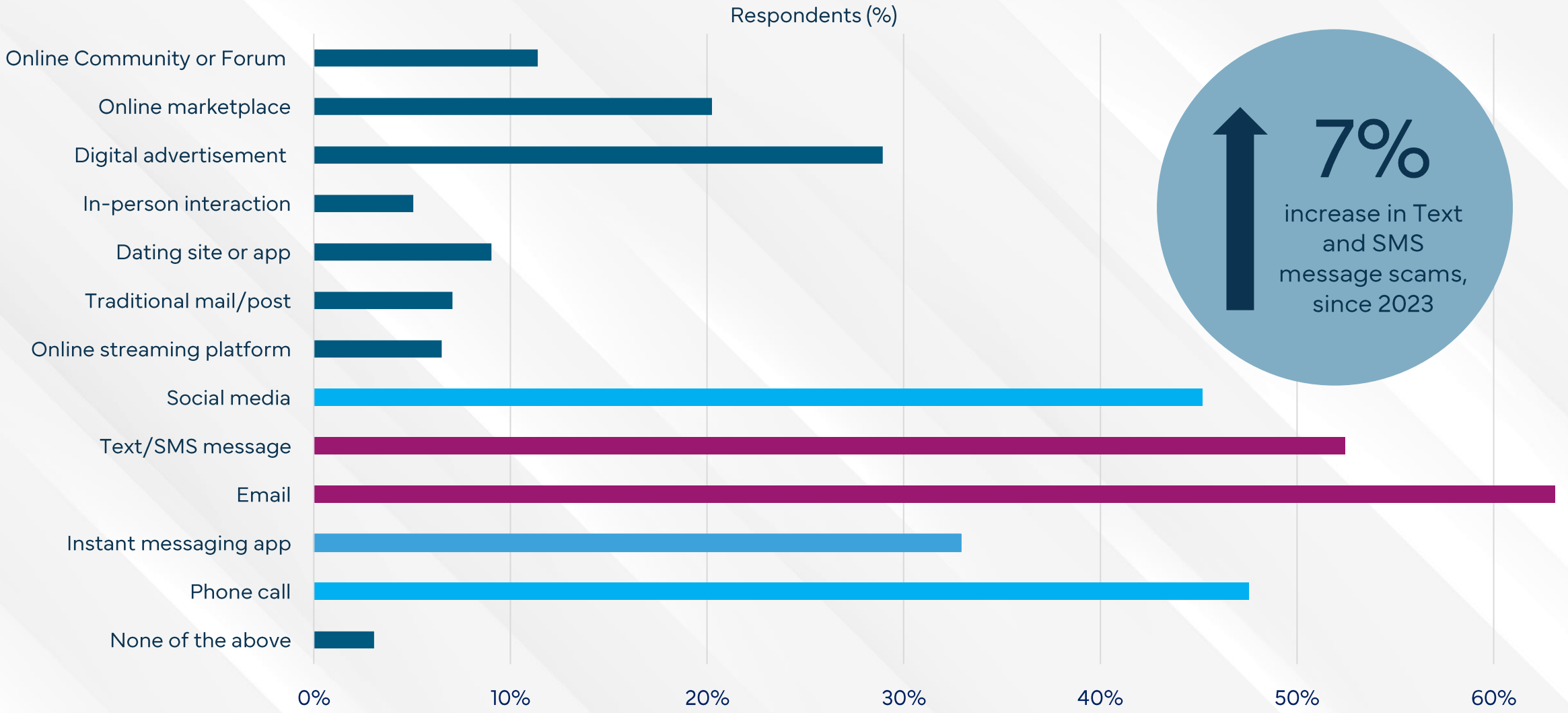
Most Swedes are aware scammers can use AI against them



Awareness of AI generated text & chats is high, while complex AI voices & images are less widely known.

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

Majority of scams are delivered via Emails or Text/SMS Messages



7%

increase in Text and SMS message scams, since 2023

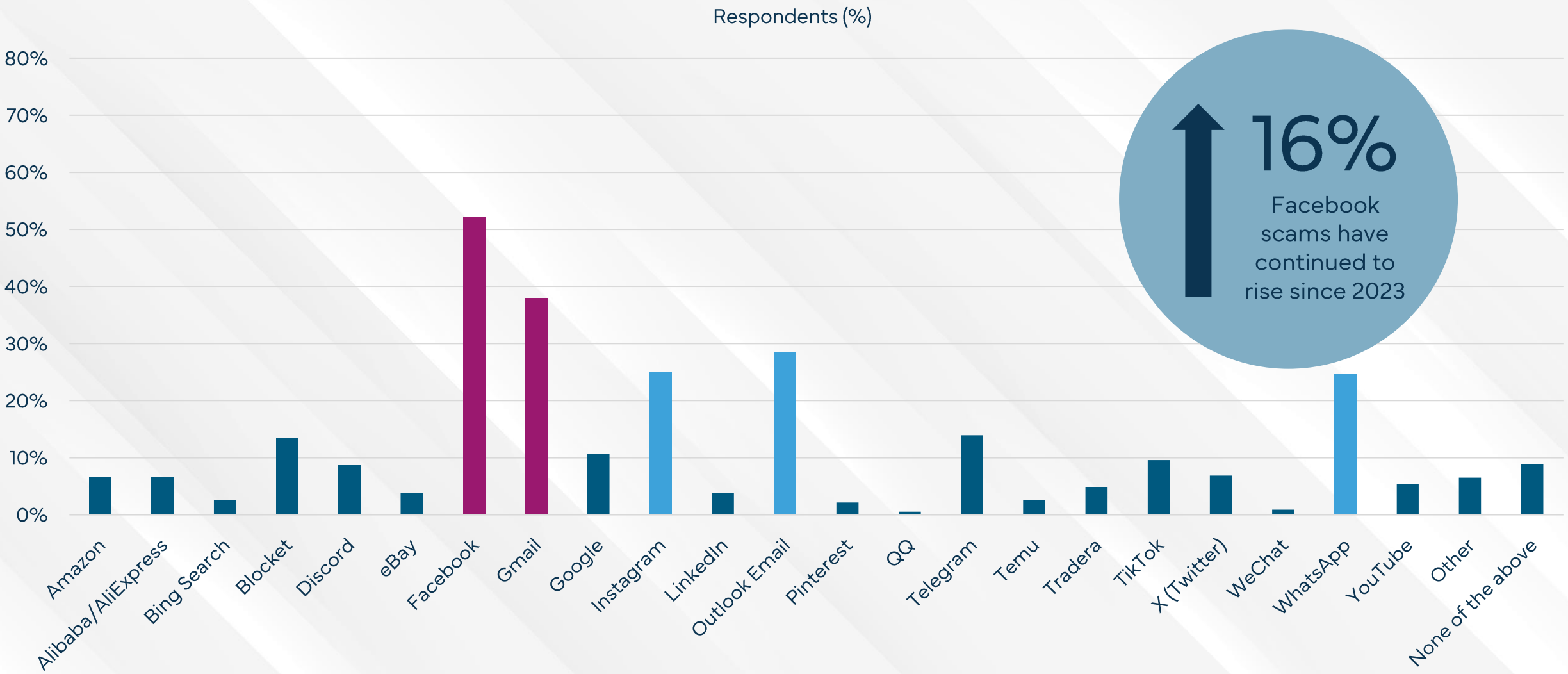
Phone calls, social media, and instant messaging apps are also common scam media.

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

Fraudsters favor Facebook & Gmail as their scam delivery platform

BioCatch

GASA
Global Anti-Scam Alliance

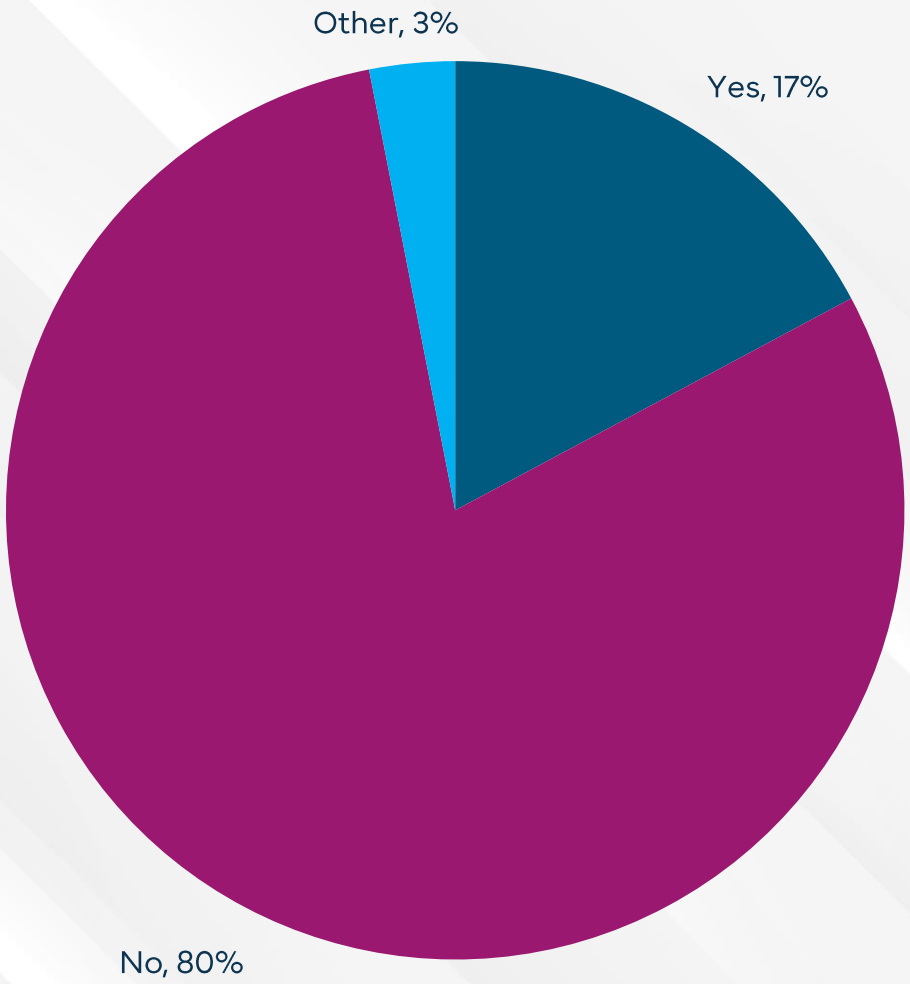


COM .NET .ORG

Outlook Email, Instagram, and WhatsApp round out the top five most popular platforms for scammers.

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

80% of Swedes did not report the scam to law enforcement

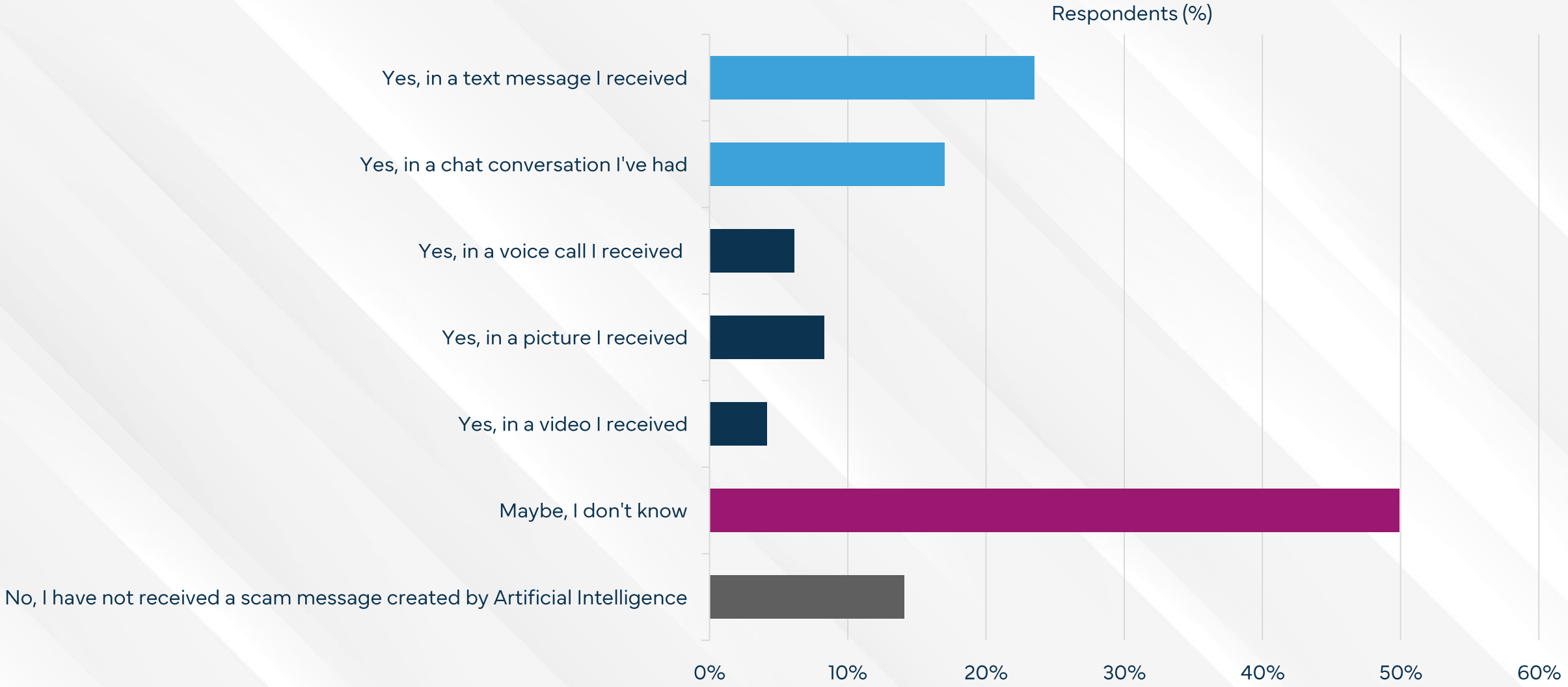


19%
decrease
in reports to law
enforcement,
since 2023

17% 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?

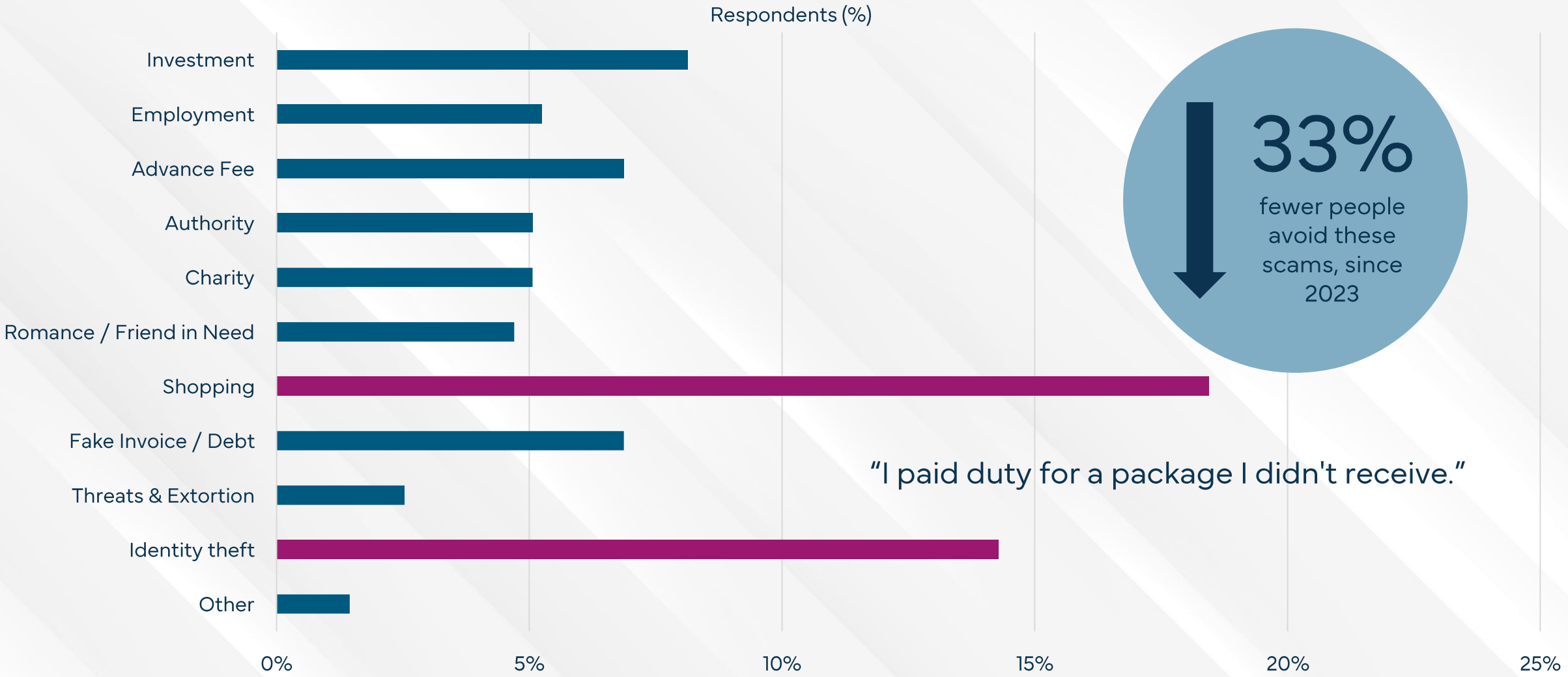
50% of Swedes were uncertain whether AI was used to scam them



14% of Swedes stated they did not believe they were subjected to scams utilizing artificial intelligence.

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

Shopping Scams are the most common type of scam in Sweden



33%
fewer people avoid these scams, since 2023

"I paid duty for a package I didn't receive."

55% did not fall victim to the most common scams in the last year. 1.66 scams were reported per victim.

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

Swedish scam victims share their stories

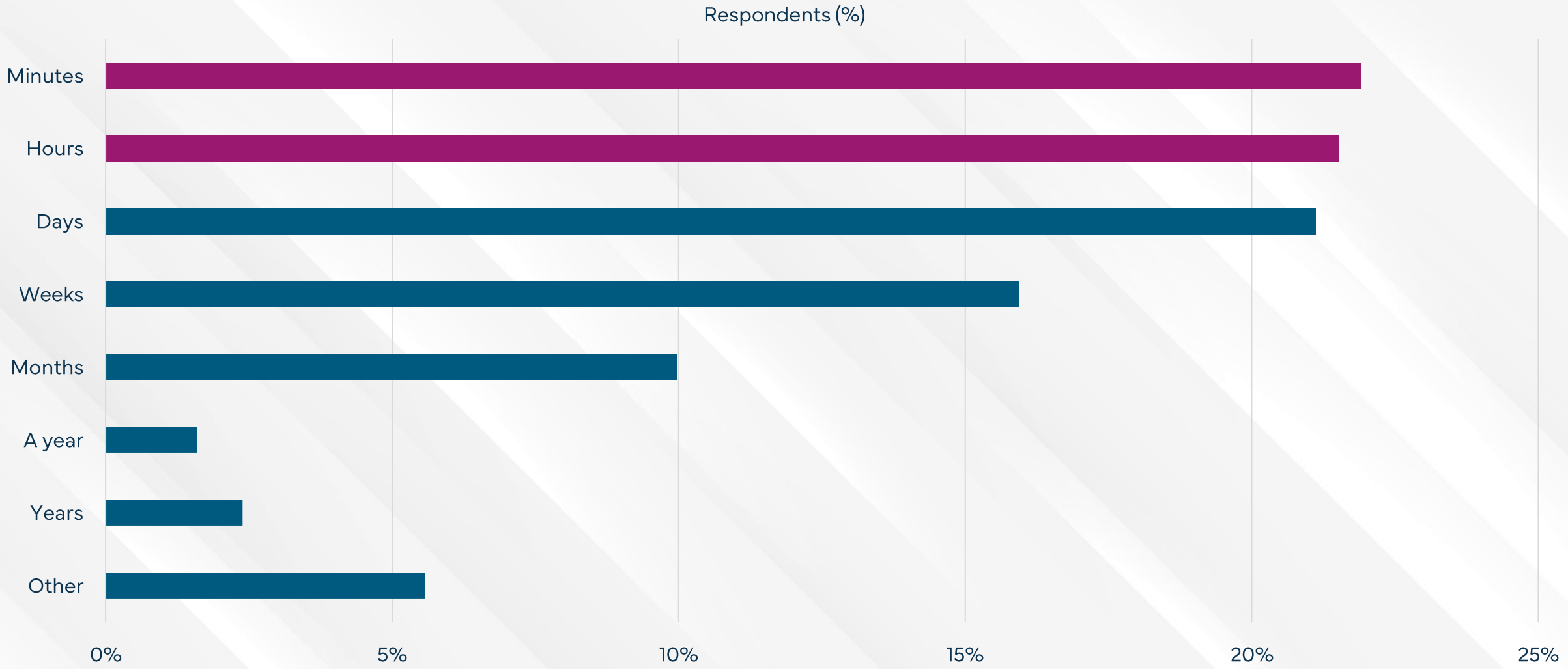
"The fraudster notified me via text message that there was a package that I would have to pay postage for, but I had not purchased the item."

"I gave money to support Ukraine, but after that I read that people took money for themselves."

"[Scammers] tricked me into a job where I would deposit money to make fake purchases so that the company would get better reviews, then get them out with a profit. It worked the first time, so I joined again and lost SEK 3,000."

"Money was withdrawn from my account without my knowledge."

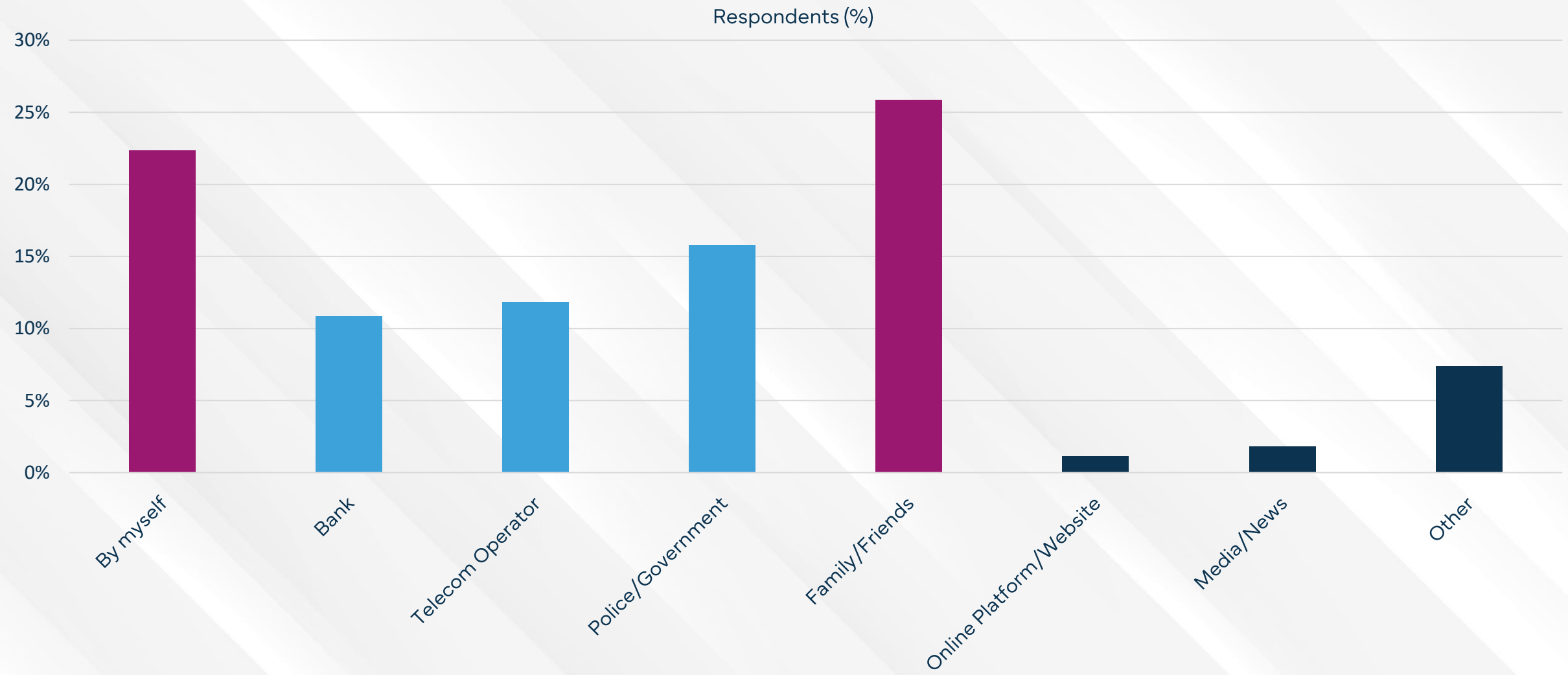
43% of scams are completed within 24 hours of first contact



22% reported scams that were over in minutes, while 4% were scammed over a year or more.

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?

1-in-4 were told by family or friends that they had been scammed

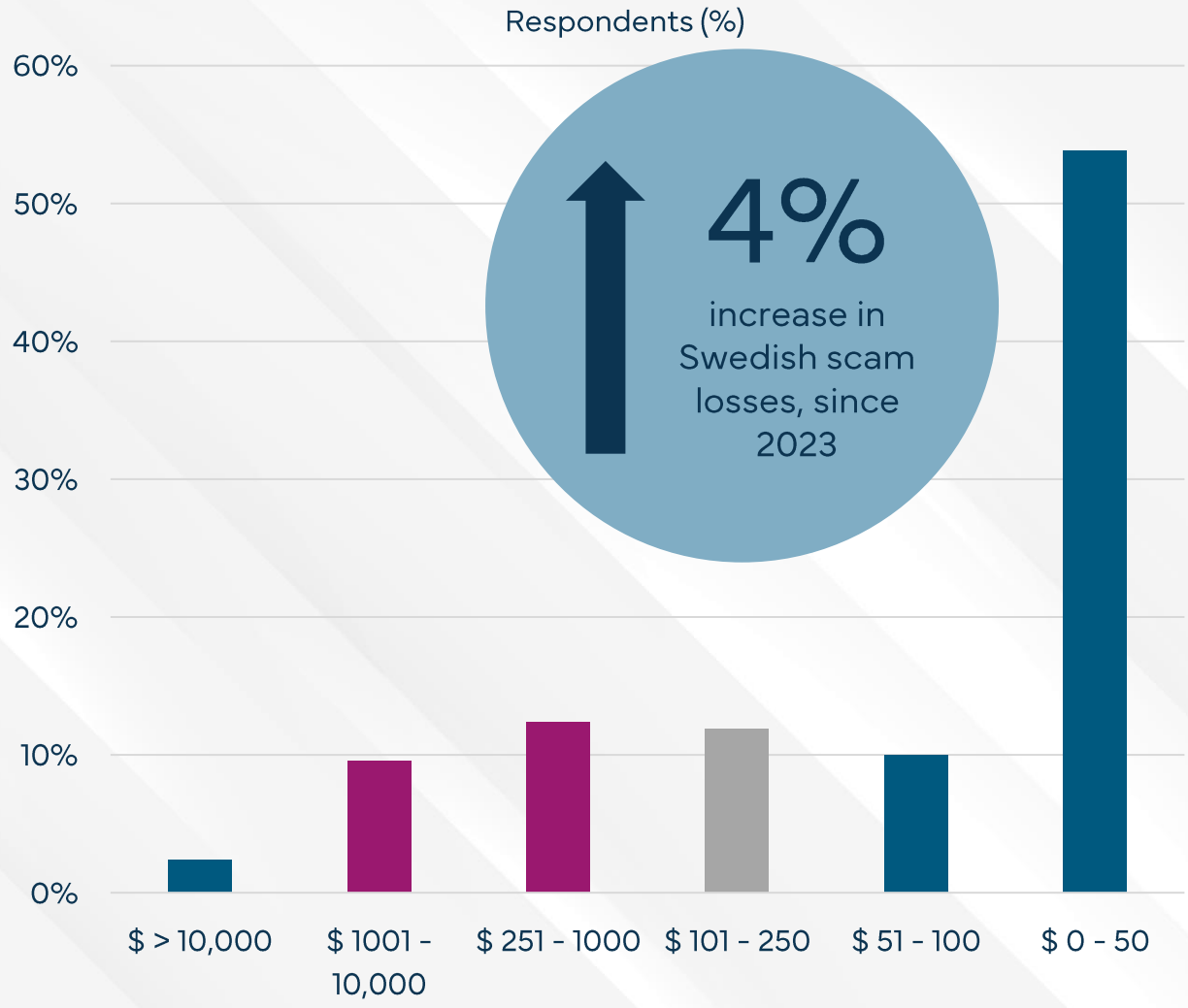


A similar number figured it out alone, while online platforms/websites are popular in pointing out scams.

Q13 How did you discover you were scammed?

In total, 12% of Swedish participants lost money in a scam

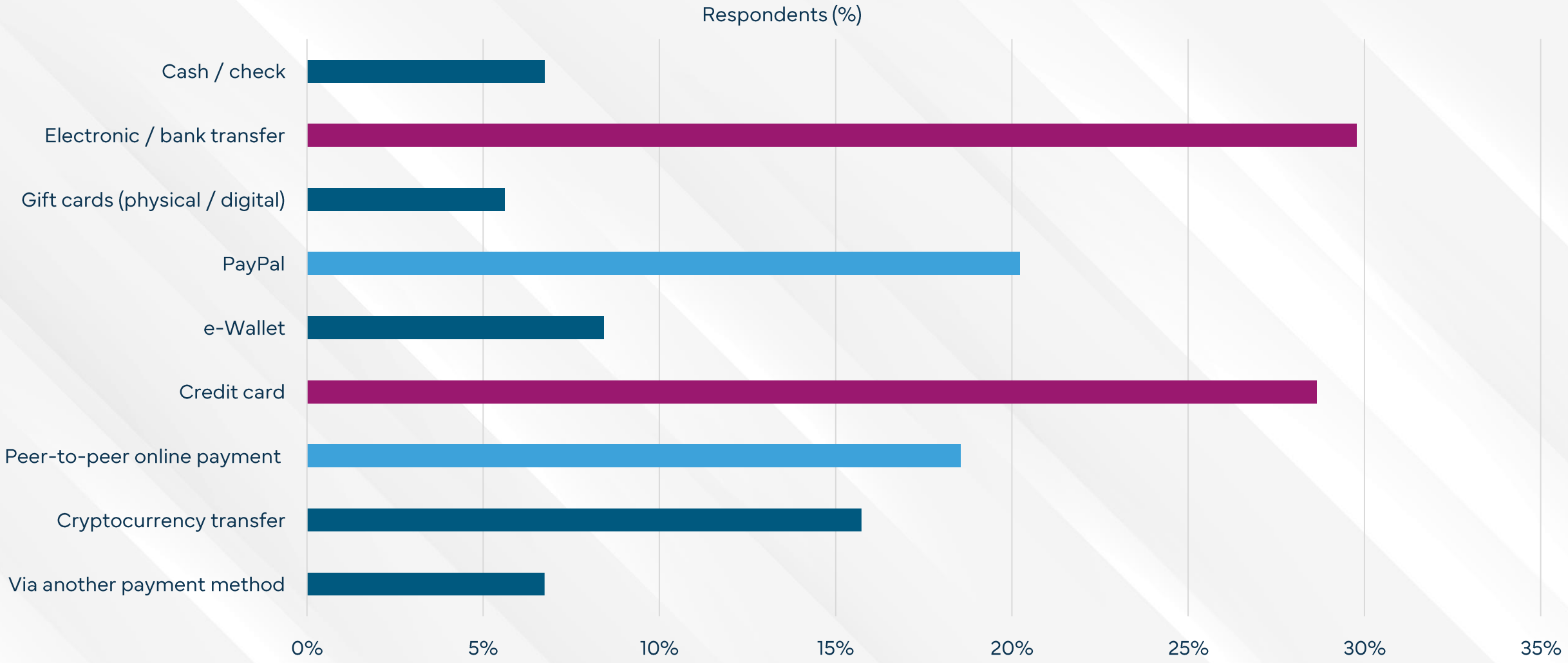
Survey Key Statistics	
Persons approached	1,284
Participants completing the survey	45%
Participants losing money	155
% losing money / approached persons	12%
Average amount lost in US Dollars	2,726
Total country population	10,536,338
Population over 18 years	8,352,039
# of people scammed > 18 years	1,007,912
Total scam losses (USD)	2,747,568,000
Total scam losses (SEK)	28,582,937,489
Gross Domestic Product (USD, millions)	597,110
% of GDP lost in scams	0.5%



In total, the Swedish lost $ 2.7 billion to scams, which is equal to 0.5% of Sweden's GDP.

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

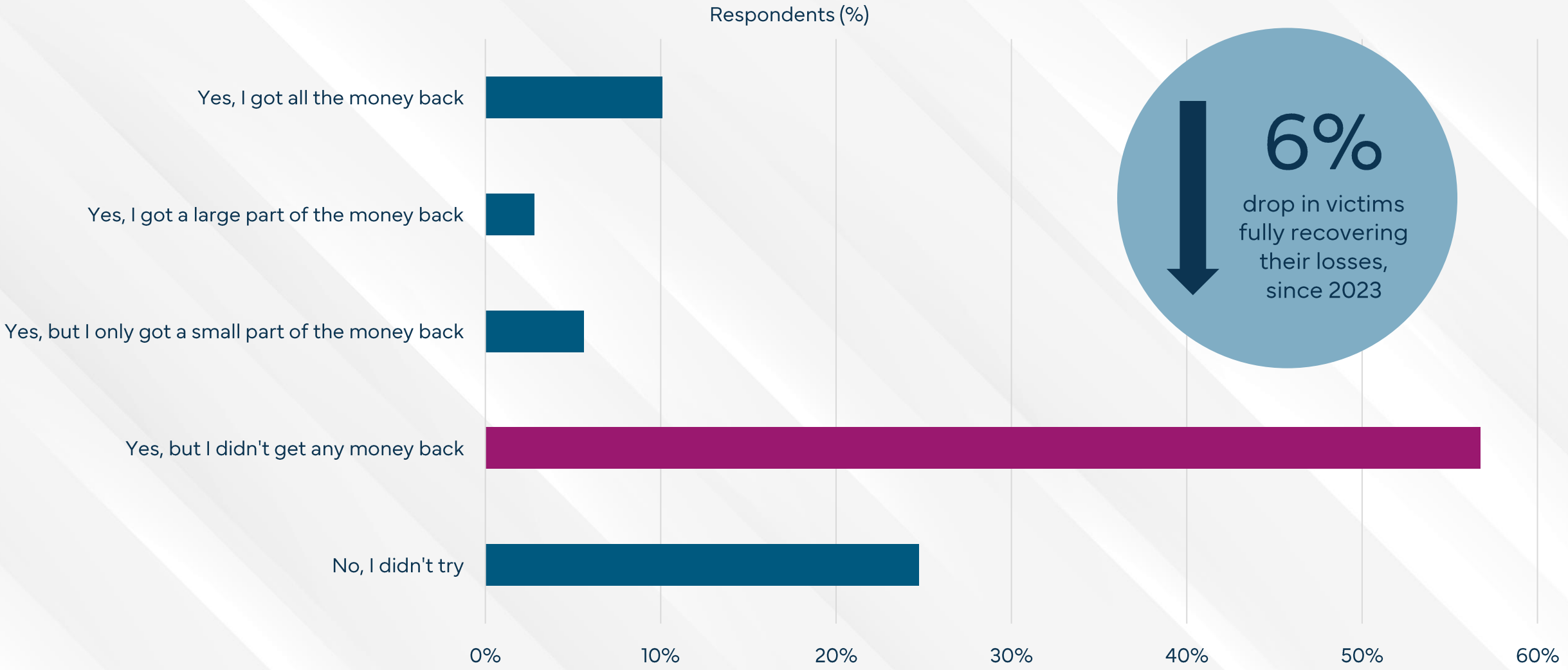
Bank Transfer & Credit Cards are the dominant payment methods



PayPal and peer-to-peer apps are also popular tools which scammers use to receive their stolen gains.

Q15 - How did you pay the scammer?

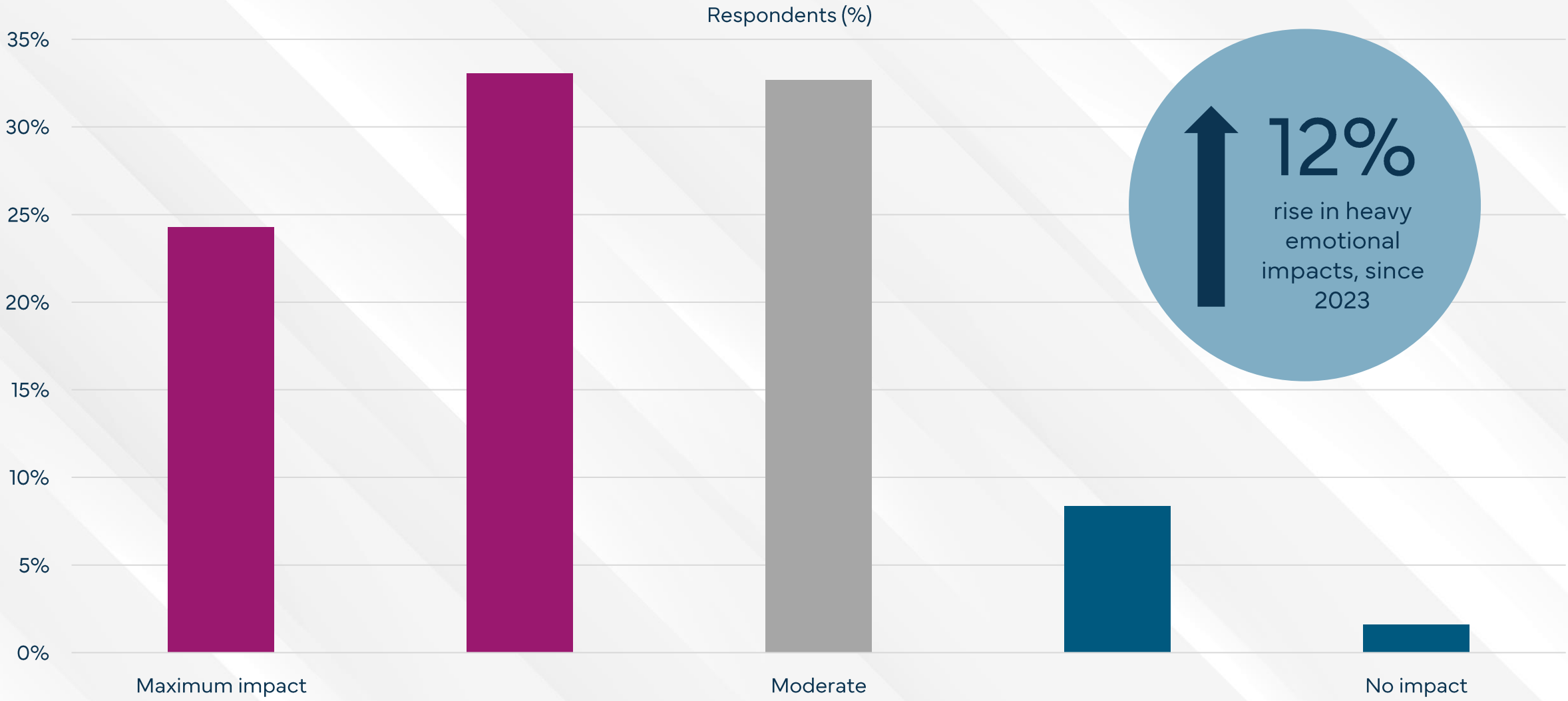
Only 10% of victims were able to fully recover their losses



25% did not try to recover their funds. 57% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

57% of the scam victims perceived a (very) strong emotional impact

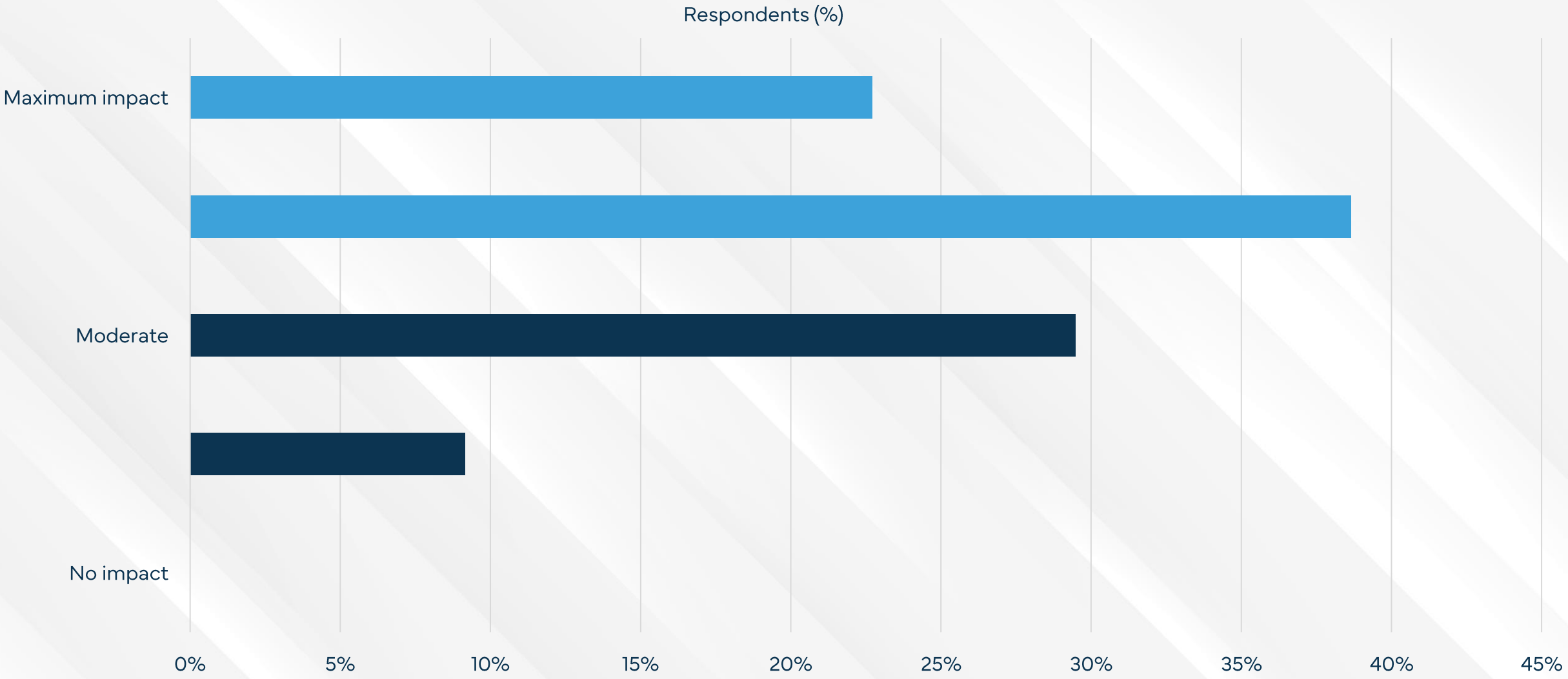


12%
rise in heavy emotional impacts, since 2023

10% of the survey respondents reported little to no emotional impact due to scams.

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

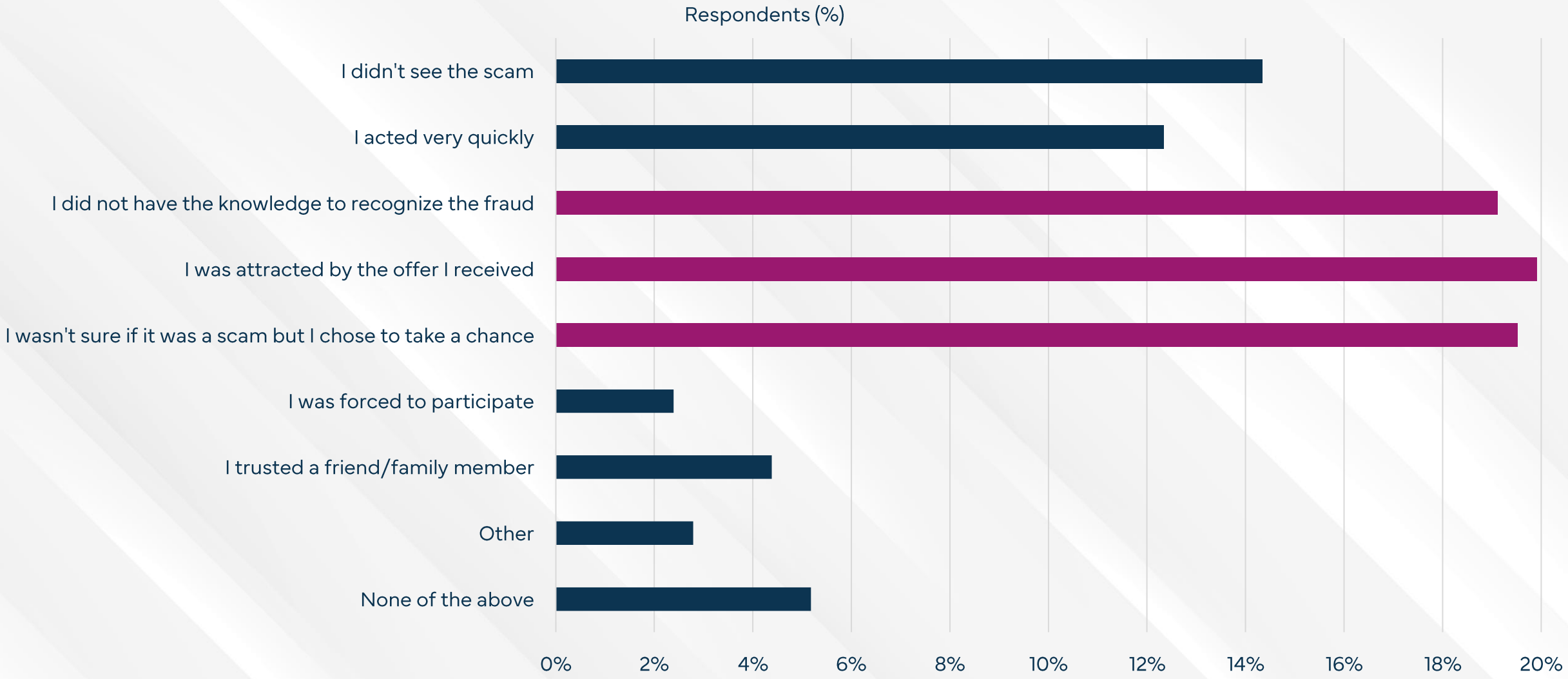
61% of Swedes have less in trust the Internet as a result of scams



Only 9% of Swedes reported little to no loss of trust in the Internet due to scams.

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

Swedes often fall for scams because the offer is so attractive



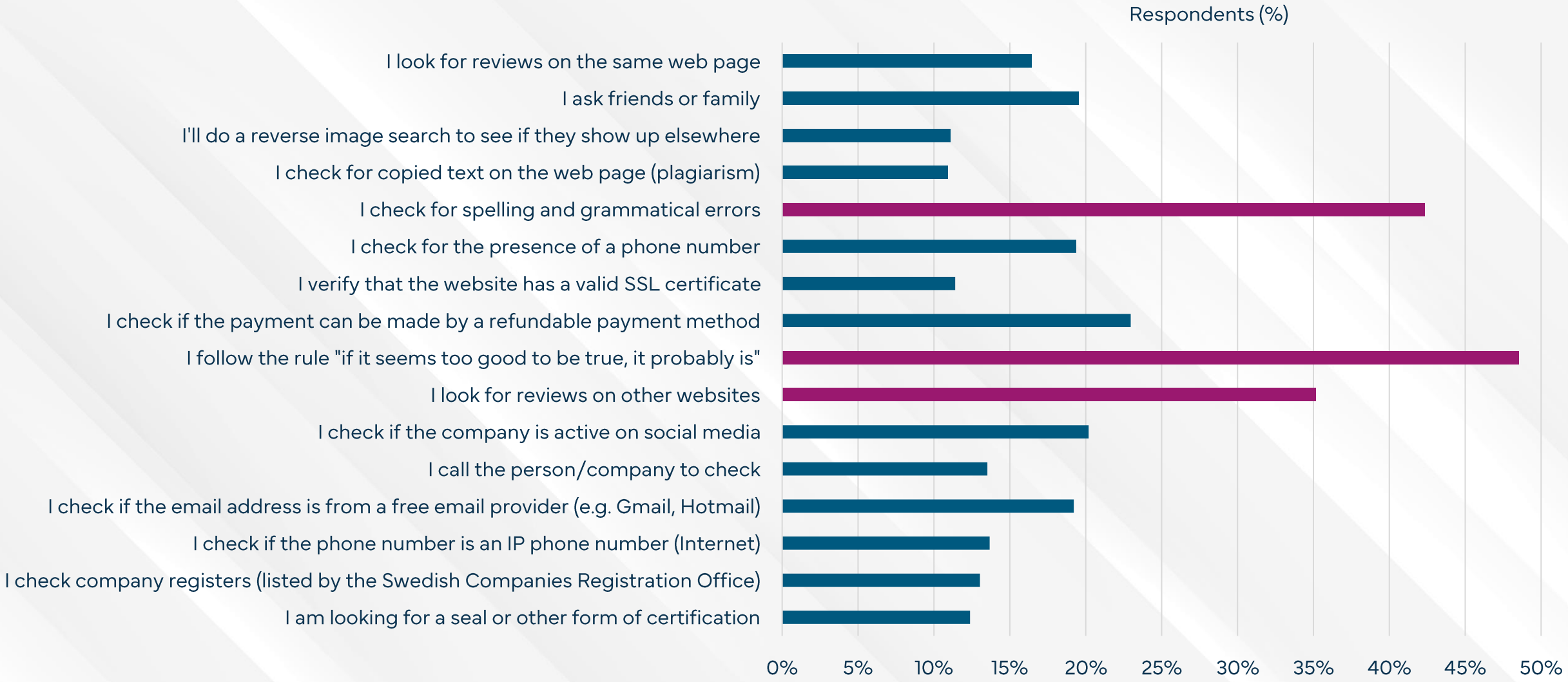
Several victims also reported uncertainty whether it was a scam while others were unable to identify it.

Q19 - What was the main reason you were deceived?

Nearly half follow the “if it is too good to be true, it probably is” rule

BioCatch

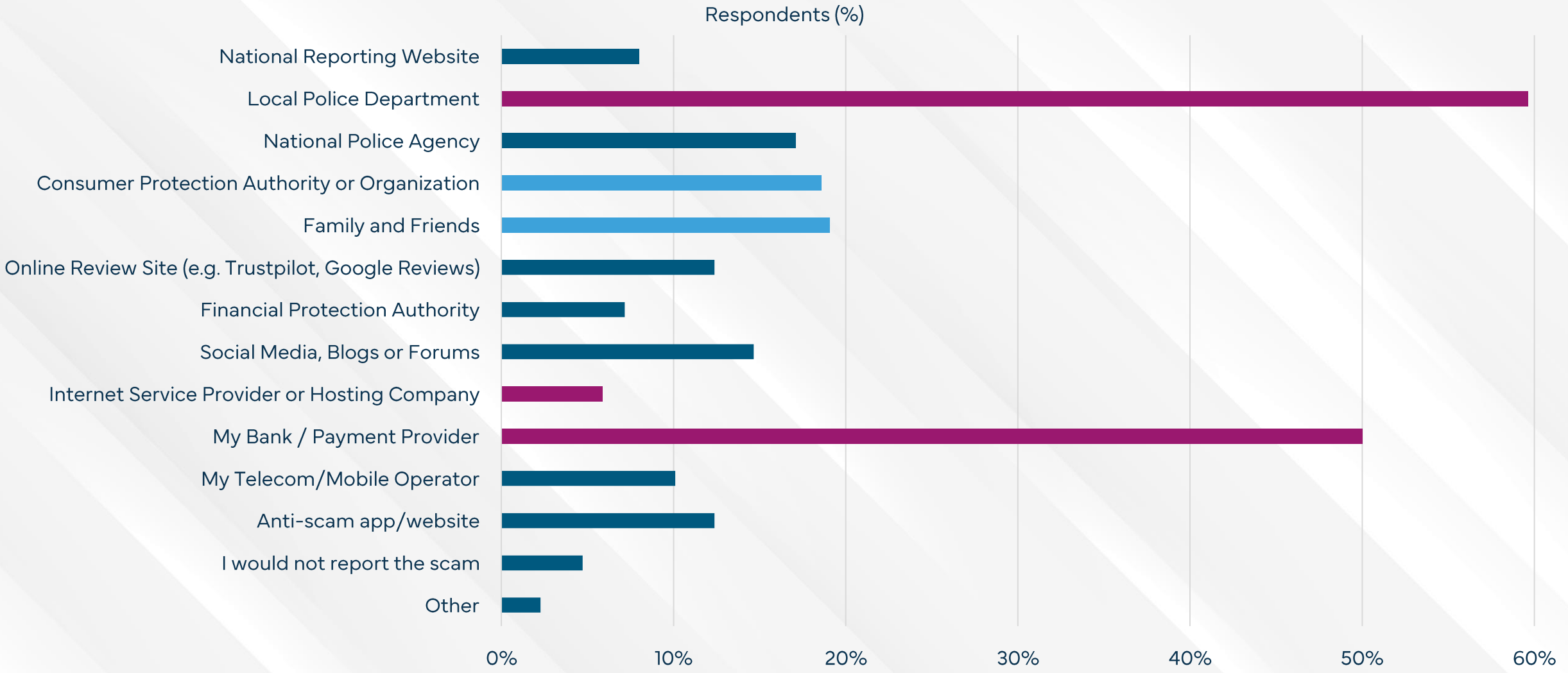
GASA
Global Anti-Scam Alliance



Many reported checking reviews on other websites and checking for spelling & grammatical errors.

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

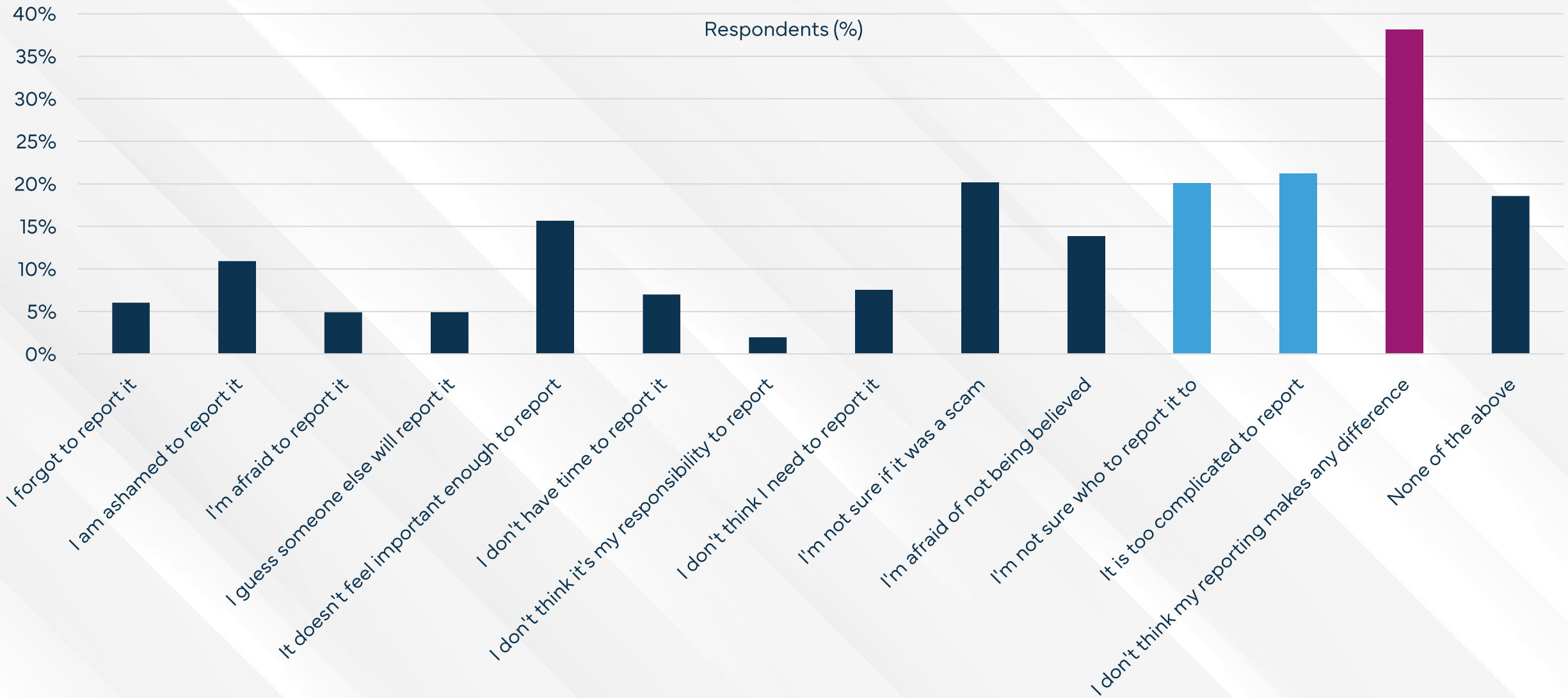
Scams are mostly shared with Local Police Stations and Banks



Family & friends, consumer agencies & general complaints board are popular places to report scams.

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

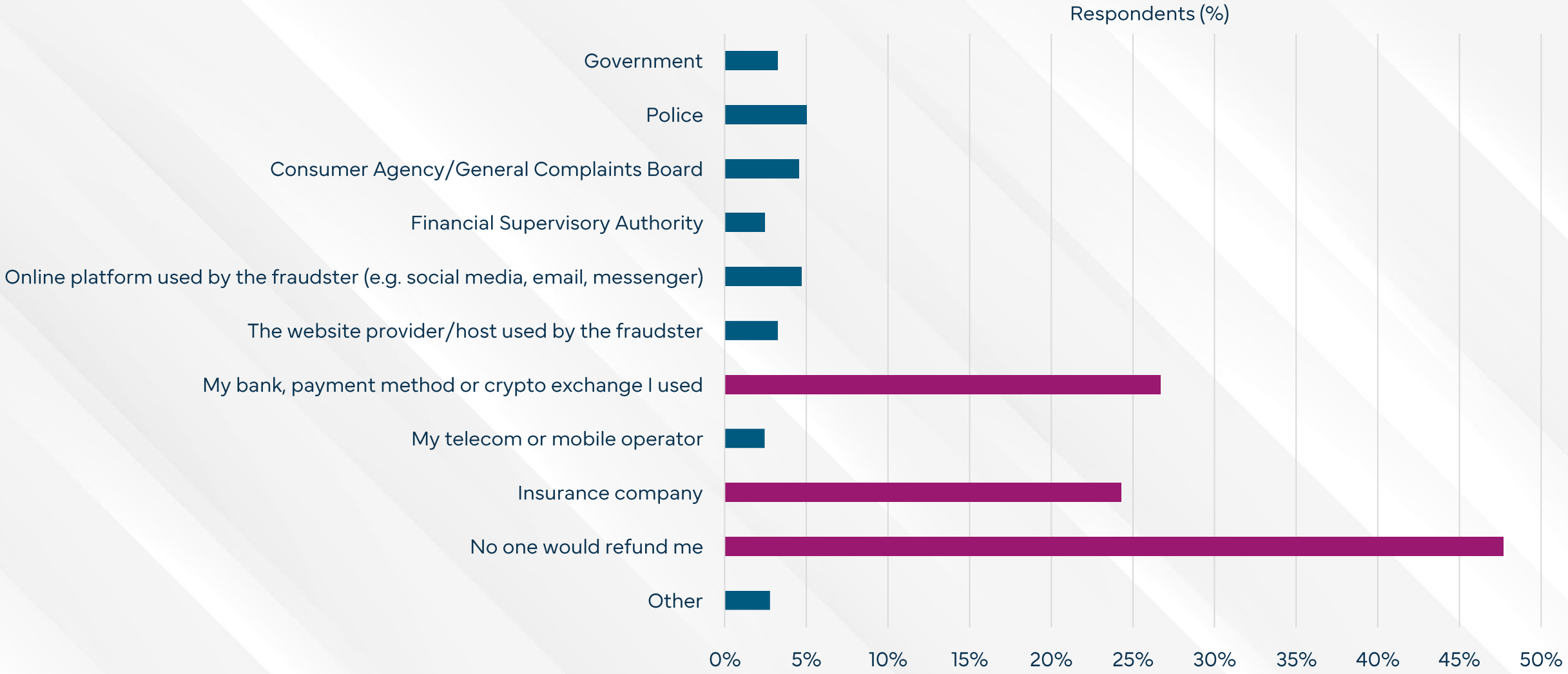
Many Swedes believe that reporting scams won't make a difference



Other reasons for not reporting are complex processes and uncertainty on where to report scams.

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

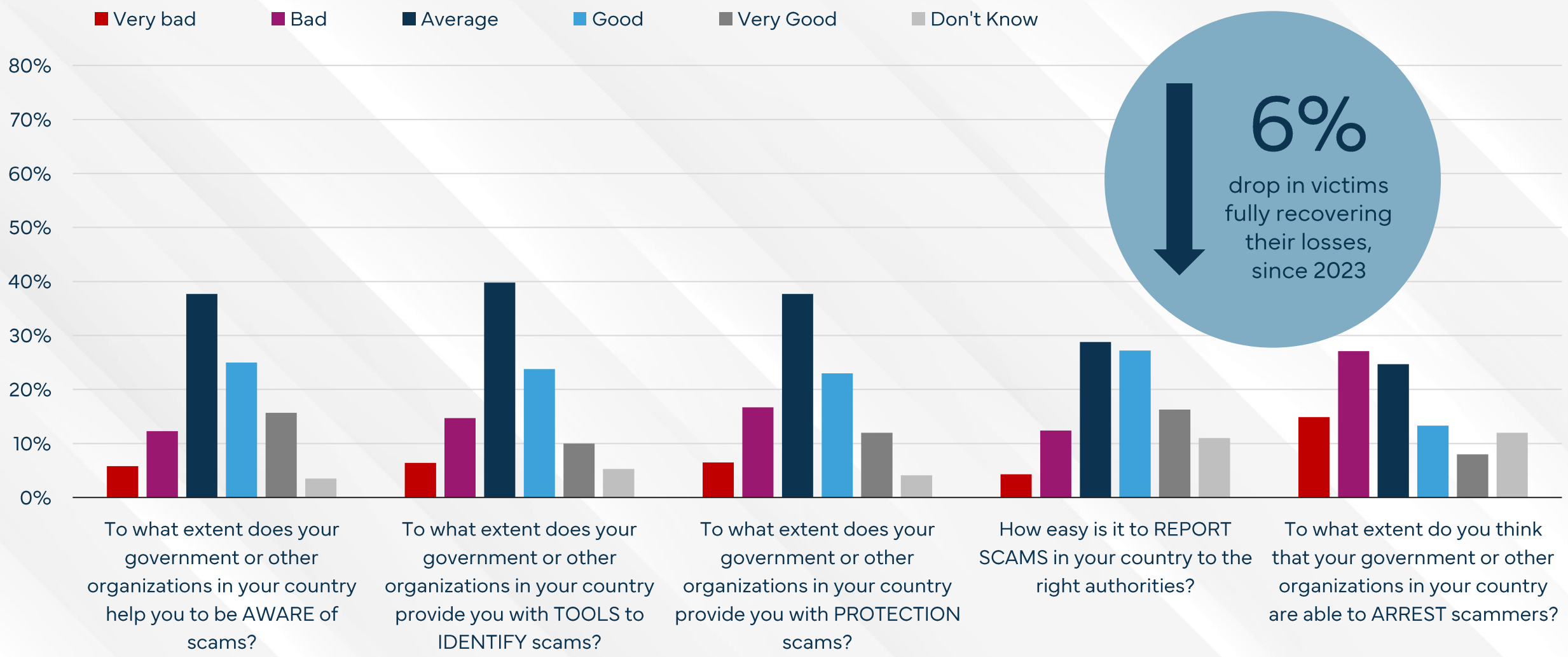
48% of Swedes assume no one will refund their scam losses



Others believe their bank, payment method, crypto exchange or insurance company will refund them.

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

Citizens are unhappy with Sweden's efforts to arrest scammers

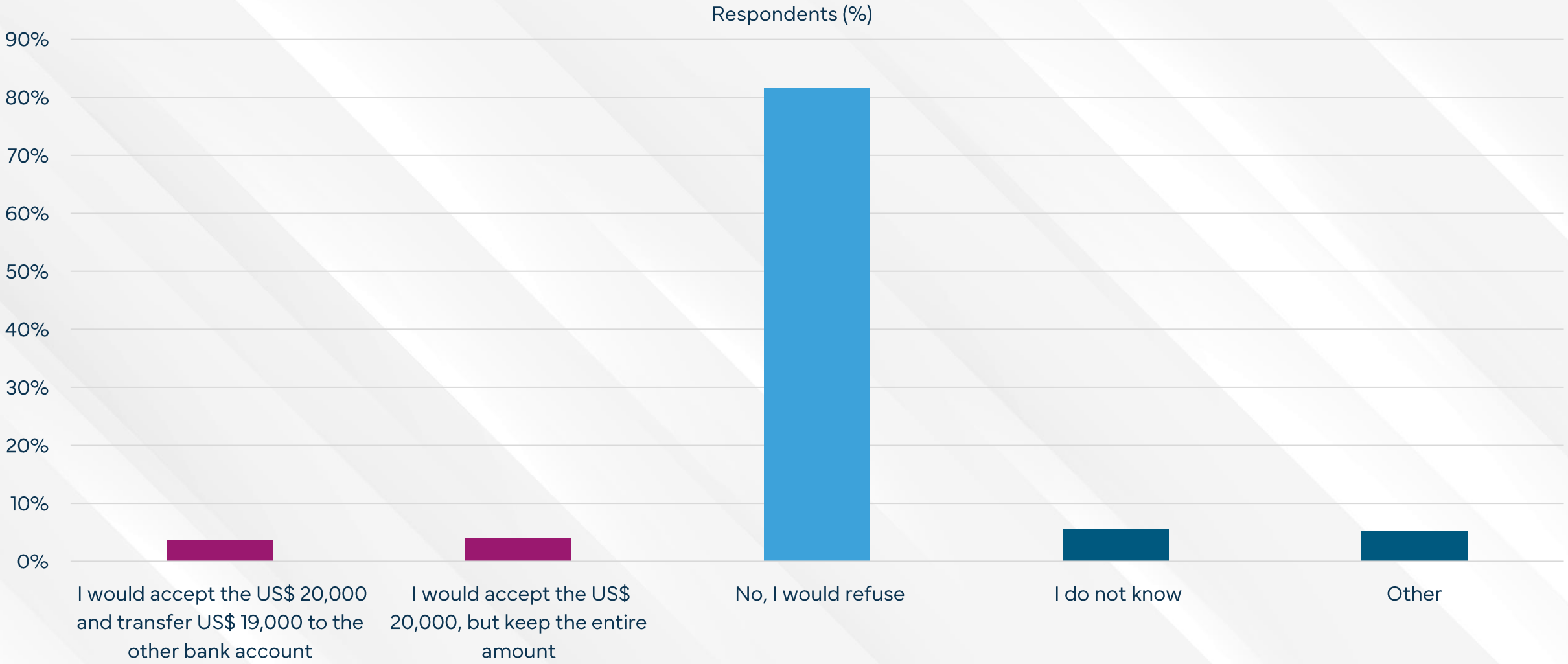


6%
drop in victims fully recovering their losses, since 2023

Overall, 24% of the participants rate the actions of governments as (very) bad, 40% as (very) good.

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?

4% of Swedes admit that they would consider being a money mule



However, 82% of those surveyed would refuse to be involved in a "money mule" scam.

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?

BioCatch

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.

At **BioCatch**, we help the world's largest, most recognizable financial institutions and telecommunication brands build trusted relationships with their customers by keeping them safe from digital fraud. We believe behaviour has become the only element of our digital identities that is truly, and uniquely, human.

SSF Stöldskyddsföreningen is a non-profit and independent association that has worked for a safer society since 1934. SSF's focus is on preventing crimes such as theft, fraud and data breaches, and is the Swedish national point of contact for the Global Anti-Scam Alliance.

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.

Sam Rogers is GASA's Director of Marketing. 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.

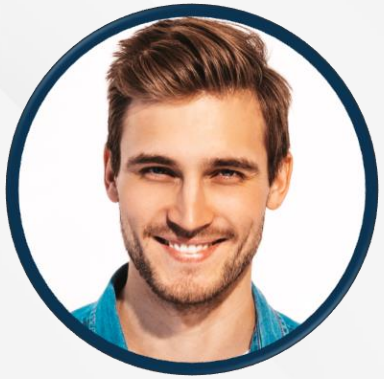
Clement Njoki is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.

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 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.



James Greening, who goes by an alias for security reasons, is the Social Media Manager at ScamAdviser and a scam investigator. He also runs the popular website Fake Website Buster.

BioCatch

Disclaimer

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

Copyright

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