feedzai

The State of Scams in The Netherlands 2024

GASA
Global Anti-Scam Alliance

1-in-7 Dutch scammed as an estimated EUR 1.75 billion vanishes in one year

The 2024 State of Scams in the Netherlands report, conducted by the Global Anti-Scam Alliance (GASA) in partnership with Feedzai, provides a comprehensive look at the current scam landscape in the Netherlands. Based on responses from 1,012 Dutch citizens, the report highlights key trends, rising threats, and the growing sophistication of scams in the country.

Confidence in identifying scams has dropped slightly, with 58% of Dutch respondents feeling sure they can recognize a scam—a 4% decrease from last year. Although 43% of the population is targeted by scams every month, 27% of respondents reported that they rarely encounter scams, indicating that scam exposure varies across the population. In the past year, scam encounters have risen for 38% of respondents, while only 19% experienced a reduction. Despite this increase, there has been an 8% overall decrease in scam encounters compared to 2023, suggesting some positive developments in scam prevention.

Awareness of AI-generated scams is growing, with many Dutch citizens familiar with AI-generated text and voices. However, knowledge of more complex AI-generated images and videos is less widespread, leaving some gaps in scam detection capabilities. The majority of scams are delivered via email or text/SMS messages, with an 8% increase in SMS scams compared to the previous year. Platforms like WhatsApp and Gmail are the most common for scam delivery, with a 1% increase in WhatsApp scams.

Scam underreporting remains a concern, with 82% of respondents opting not to report scams to law enforcement—a 9% increase from last year. Among those who did report scams, banks and local police were the most popular channels.

Shopping scams remain the most common type of fraud in the Netherlands, followed by a spike in romance scams over the last year. Scam victims in the Netherlands tend to be retargeted, with an average of 0.7 scams reported per victim. Many Dutch citizens shared stories of being targeted through email, investment scams, and online shopping fraud, with scammers often completing their schemes within 24 hours of first contact.

Financially, the Dutch have lost an estimated US$1.94 billion (EUR 1.75 billion) to scams in 2024, equivalent to 0.2% of the country's GDP. The average amount lost per victim was $938. Only 6% of victims were able to fully recover their losses, reflecting a slight drop in recovery rates compared to last year. A quarter of victims did not attempt to recover their funds, and 55% of those who tried were unsuccessful.

The emotional toll of scams is notable, with 42% of respondents reporting a strong emotional impact, though this figure has decreased by 6% since 2023. Nearly half of the Dutch population has lost trust in the internet due to scams, while 25% reported little to no emotional impact.

Many Dutch citizens fall victim to scams because they act quickly on tempting offers or fail to recognize warning signs. Despite this, nearly half of respondents adhere to the "if it seems too good to be true, it probably is" rule, and many take steps to verify scam risks by checking for typos, grammatical errors, and online reviews.

The State of Scams in the Netherlands 2024 report shows that while awareness of scams is growing, the prevalence and sophistication of scams continue to present a serious challenge. The Dutch government and financial institutions must improve public education on scam recognition, streamline reporting processes, and enhance support for victims seeking to recover their losses.

Greater collaboration between law enforcement, banks, and tech platforms is essential to reduce the impact of scams on Dutch citizens. By increasing public awareness, simplifying reporting mechanisms, and bolstering legal frameworks, the Netherlands can take meaningful steps toward mitigating the threat of scams and restoring public trust in online and digital interactions.

Jorij Abraham
Managing Director

GASA
Global Anti-Scam Alliance

Sam Rogers
Director of Marketing

Tackling the Rising Threat of Fraud in the Netherlands: Insights from Fraude Helpdesk on Scams and Consumer Protection Strategies

How significant has the issue of scams become in the Netherlands?

The Fraude Helpdesk is the national reporting center for fraud in the Netherlands. Our goal is to minimize the financial and emotional impact of fraud by providing a low-threshold, personal, and accessible helpdesk for those affected. We receive approximately 60,000 reports annually through our front office, and around 600,000 suspicious emails are forwarded to us for automated checks. However, not everyone reports fraud. Research shows that 1 in 6 Dutch citizens has been a victim of fraud.

What types of scams have trended in the Netherlands recently?

One of the most prominent types of fraud we see is what we call "bank helpdesk fraud." This scam typically starts with a phone call from a fake bank employee. The imposter claims there is a digital or financial threat, which supposedly requires the victim's (savings) money to be transferred to a special "safe" account. These fake employees often come to the victim's home afterward to collect the bank card and sometimes even take valuable items, allegedly for safekeeping at the bank. People aged 55 and over are particularly targeted in this way. The continued success of this type of fraud may be due to a relatively new tactic: victims often first receive a phishing email requesting personal details such as their name, bank account number, and phone number. Once the victim submits this information, they receive a call from the "bank employee" who tells them that their account is under threat, possibly due to the phishing email they responded to earlier. Victims often believe this because they already had doubts about the email. In 2023, this method resulted in financial losses amounting to 28 million euros, according to bank figures.

Investment fraud has also led to a sharp increase in reported financial losses. In the first six months of 2024, 14 million euros in losses were reported to us—almost as much as was reported during the entire year of 2022. A key factor behind this surge is the sophisticated combination of investment fraud with dating fraud: a so-called online dating partner cleverly persuades the victim to start investing. This process is often referred to as "pig butchering."

Another striking method leading to significant financial losses per victim is fraudulent home-based work schemes. People interested in earning extra money from home are recruited to perform "tasks" via an online platform. These tasks typically involve reviewing or assessing products or services they haven't actually used. If the home workers do not complete enough tasks within a set time, they are required to pay a fee. Sometimes they are promised additional earnings if they invest their own money. There is also the possibility of investing in cryptocurrencies online, where a seemingly large profit is displayed in their online account. However, this profit or salary is never paid out because the entire setup is fake. Not only does this impose a financial burden on the home workers, but it also erodes trust in online reviews, as these individuals inadvertently contribute to misleading other consumers. As a result, some victims may be hesitant to report their experience to us after realizing they've been scammed.

There are various campaigns where both public and private entities collaborate. By combining our knowledge and reaching a wider range of target groups, we can achieve more. It is crucial that we deliver a clear message and offer a simple, actionable, and easy-to-remember course of action.

What further actions could give consumers the upper hand in fighting scams?

The Fraude Helpdesk aims to minimize the impact of financial-economic fraud on victims as much as possible. By offering a one-stop shop and fostering close cooperation between the Fraude Helpdesk, the criminal justice system, and other partners, we can ease the burden on victims, provide better assistance, and facilitate detection and prosecution—a win-win situation. To accomplish this, it is necessary that we receive complete reports, including (screenshots of) false messages and, for instance, the bank account numbers to which money has been transferred. This will require either an amendment to the privacy law or the granting of permission for us to process this data. Ultimately, I believe this will benefit everyone.

Henriëtte Bongers LL.M
Managing Director
Fraude Helpdesk

FRAUDEHELPDESK.nl

Banks Must Unite to Stop the 'Normalisation' of Scams

Consumers in the Netherlands lost an extraordinary sum (EU1.75 billion) to scams last year, as outlined in The State of Scams in the Netherlands 2024 report. That averages to about $938 lost per case with only 6% of victims able to fully recover their lost funds.

These enormous losses may not be the most unsettling element outlined in GASA's Netherlands report. What's more concerning perhaps is that the report shows how consumers are becoming increasingly normalised against the impact of scams.

For example, 42% of Dutch scam victims said they were strongly emotionally impacted by being scammed. That's a 6% drop compared to the previous year. Unfortunately, it may be a sign that consumers are growing accustomed to scams and their effects. It's difficult to assess if this is an outlier, or an indication that consumers are becoming normalised to scams as part of normal life.

The report also found that 4% of Dutch citizens expressed openness to acting as a money mule. Applied to the full Netherlands population (approximately 18 million), that amounts to 720,000 people. Meanwhile, another 4% said they would keep any money given to them for themselves, a risky move that could land them in the crosshairs of criminal gangs.

This is not the only way that consumers' attitudes toward scams appear to be changing. GASA also found Dutch consumers are slightly less confident that they can identify a scam, with a 4% drop reported from the previous year. This may be the result of scammers' tactics growing increasingly sophisticated and incorporating tools like Generative AI to mimic voices, create images, or draft clear, convincing texts and emails. Still, a majority of respondents (58%) expressed confidence they could spot a scam.

Consumer views on scams are shifting, but not in the preferred direction. It appears consumers are either becoming more numbed to the effects of scams or even willing to participate in criminal activity as GASA's data on money mule participation indicates.

Banks need a cross-industry coalition to guard against criminals, to keep consumers safe from scams, to educate them on the risks of money mule activity, and to stop the "normalisation" of scam losses before it expands. Increased collaboration is needed among banks, financial institutions, and organisations outside the financial services sector. A majority of scams in the Netherlands begin by email, messages, and by phone calls (an 8% increase from last year). This pattern should be a prompt for change for financial services, telecoms, and email service providers, who play a critical role in connecting scammers with their victims.

Financial institutions should also look to collaborate with each other on stopping scams. Much of the focus on scams has been on funds departing a bank account. However, receiving banks have an opportunity to catch scam profits that are transferred to their organisation. Focusing on inbound payments opens new doors to raise the rate of recovered funds above 6%. Scam reimbursement is mandatory in the UK with sending and receiving organisations splitting the losses evenly. Voluntarily implementing a policy or forming a framework for reimbursement would be a significant distinction feature for any bank that operates without a mandate.

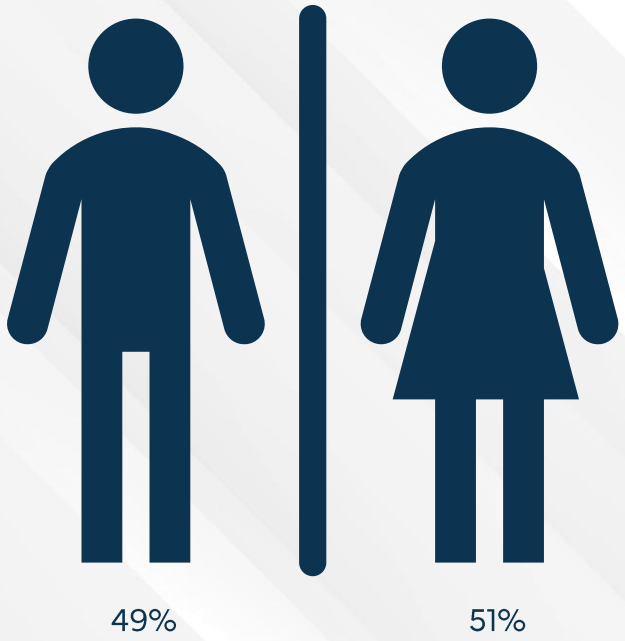
Collaboration is critical to keeping consumers safe from scams. Feedzai is proud to support GASA's collaborative initiative to foster improved engagement and partnership between telecoms, social media platforms, email providers, and cybersecurity firms, to band together against scam threats with education, sharing critical information and experiences. We are excited to share these insights on how Dutch banks learn from similar scam prevention efforts and turn the tide against scams.

Scams should not be treated as a "normal" part of everyday life. Through our partnership with GASA we can foster a collective, cross-industry commitment to doing what is right for consumers; creating a safer online environment, and reducing scam risk at every digital interaction and touchpoint.

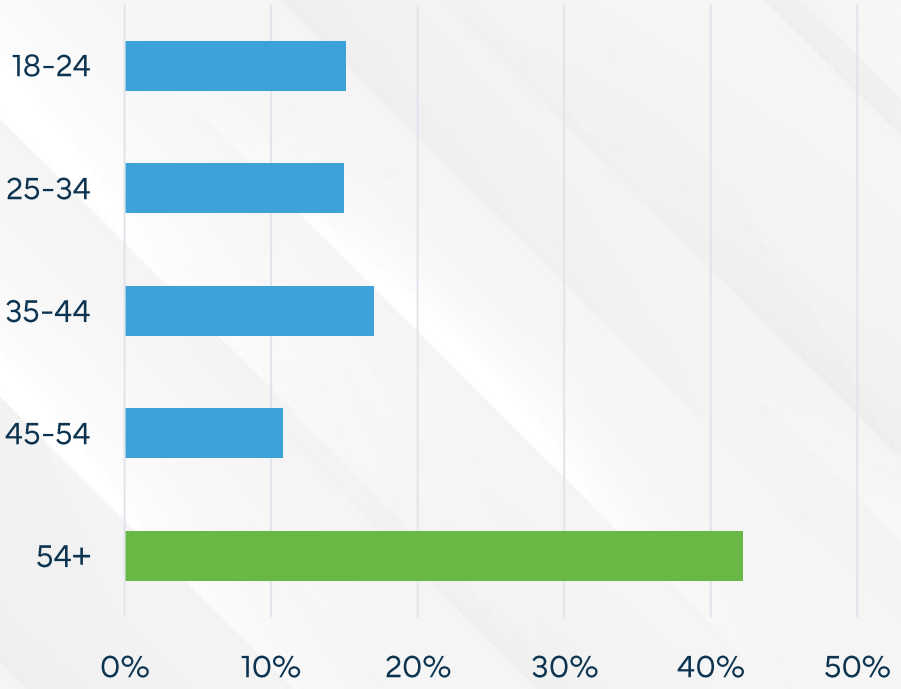
Dan Holmes
Director of Banking,
Identity & Market Strategy
Feedzai

1,012 Dutch completed the State of Scams in Netherlands survey

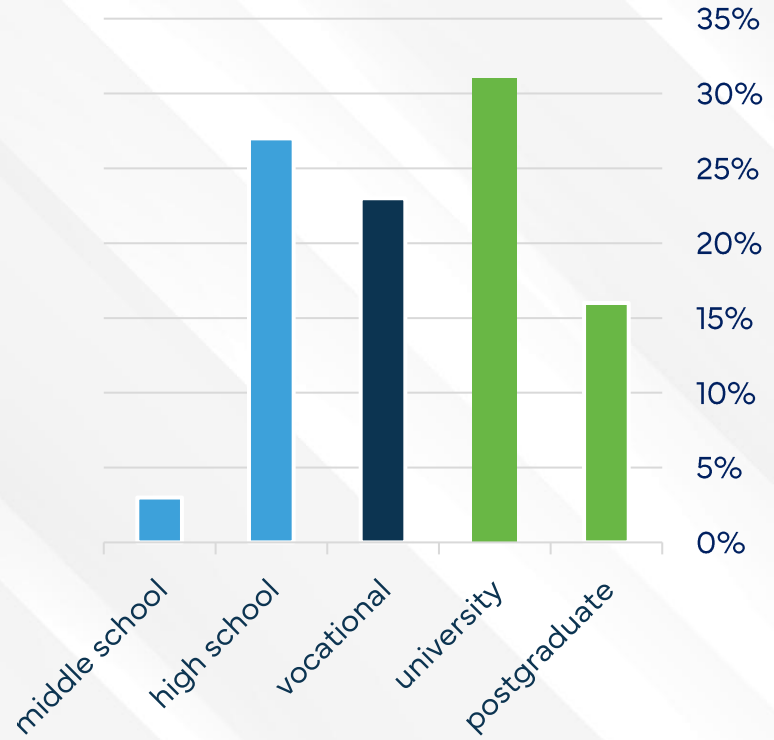
Gender



Age Range

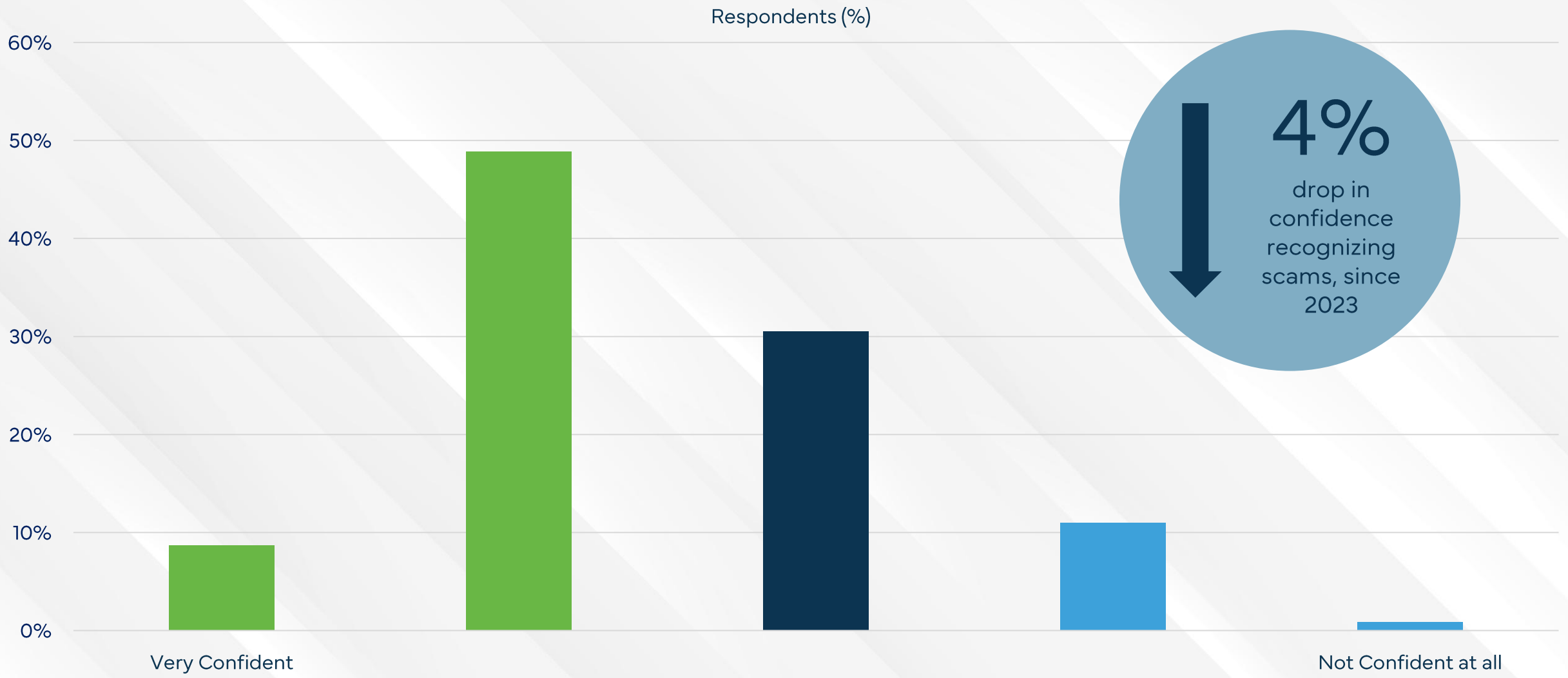


Education



The demography of respondents to the State of Scams in Netherlands 2024 survey consists of slightly more women than men. A large proportion were between 25-34 years,.

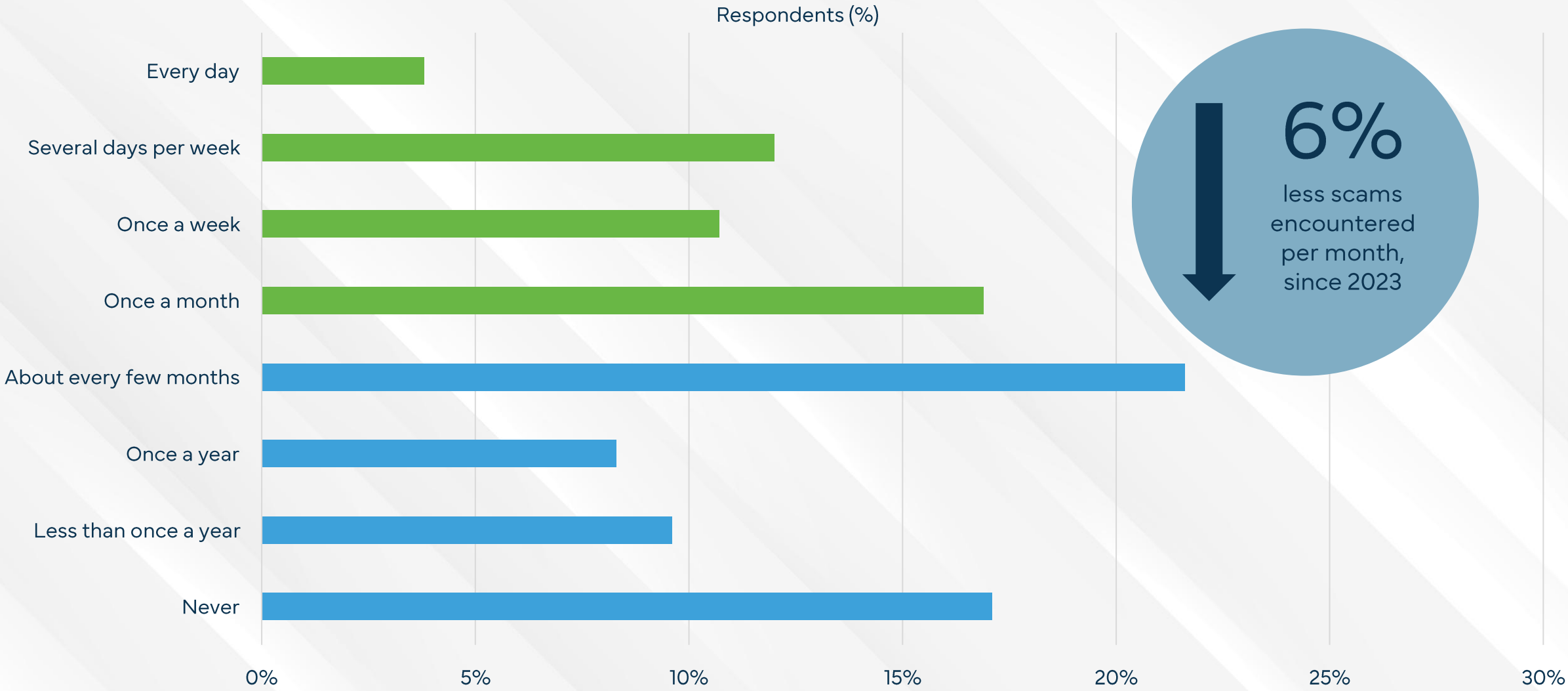
58% of people in the Netherlands are sure they can identify scams



Only 12% of respondents do not trust in their own ability to reliably identify scams.

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

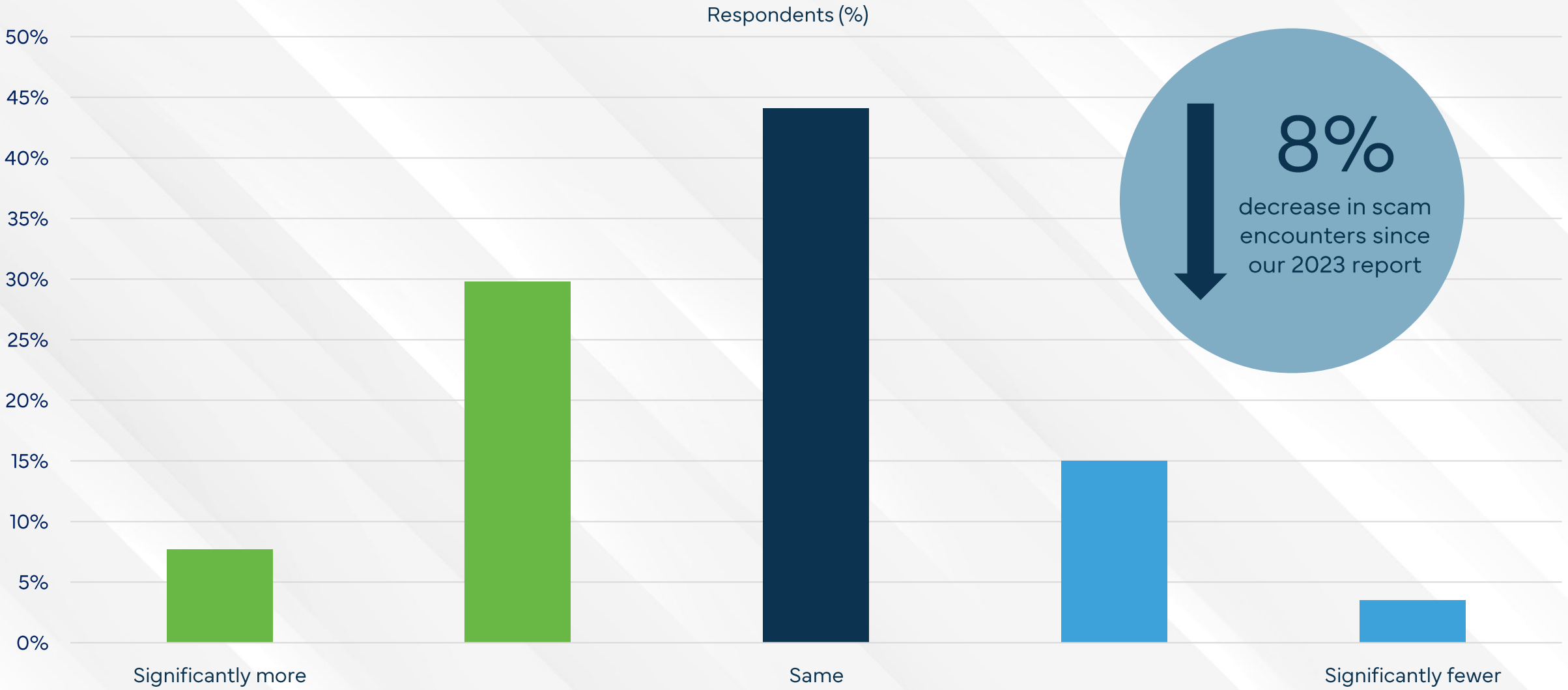
Each month, 43% of people in the Netherlands are targeted by scams



27% of Dutch survey respondents revealed that they are rarely confronted by scams.

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.

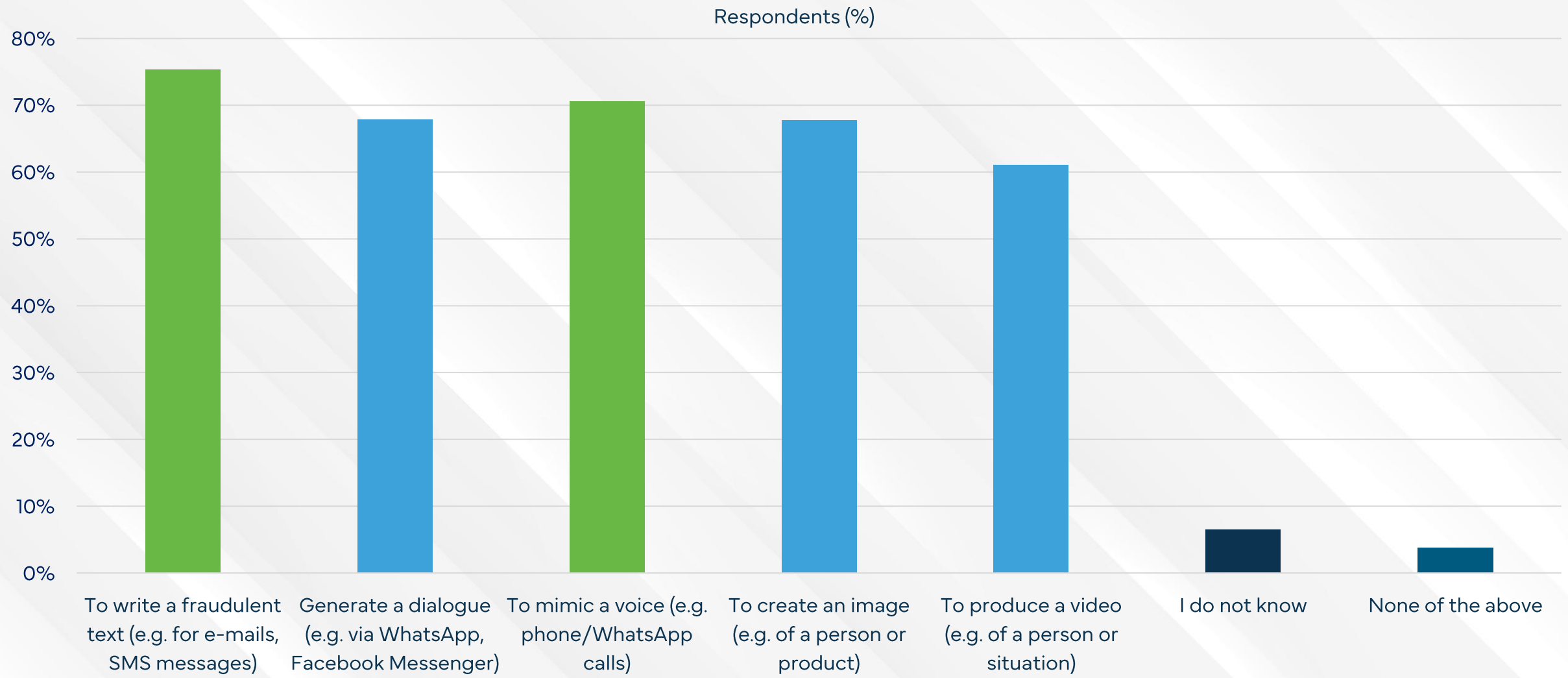
Scam encounters have risen for 38% of the Dutch in the past year



Only 19% of Dutch 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?

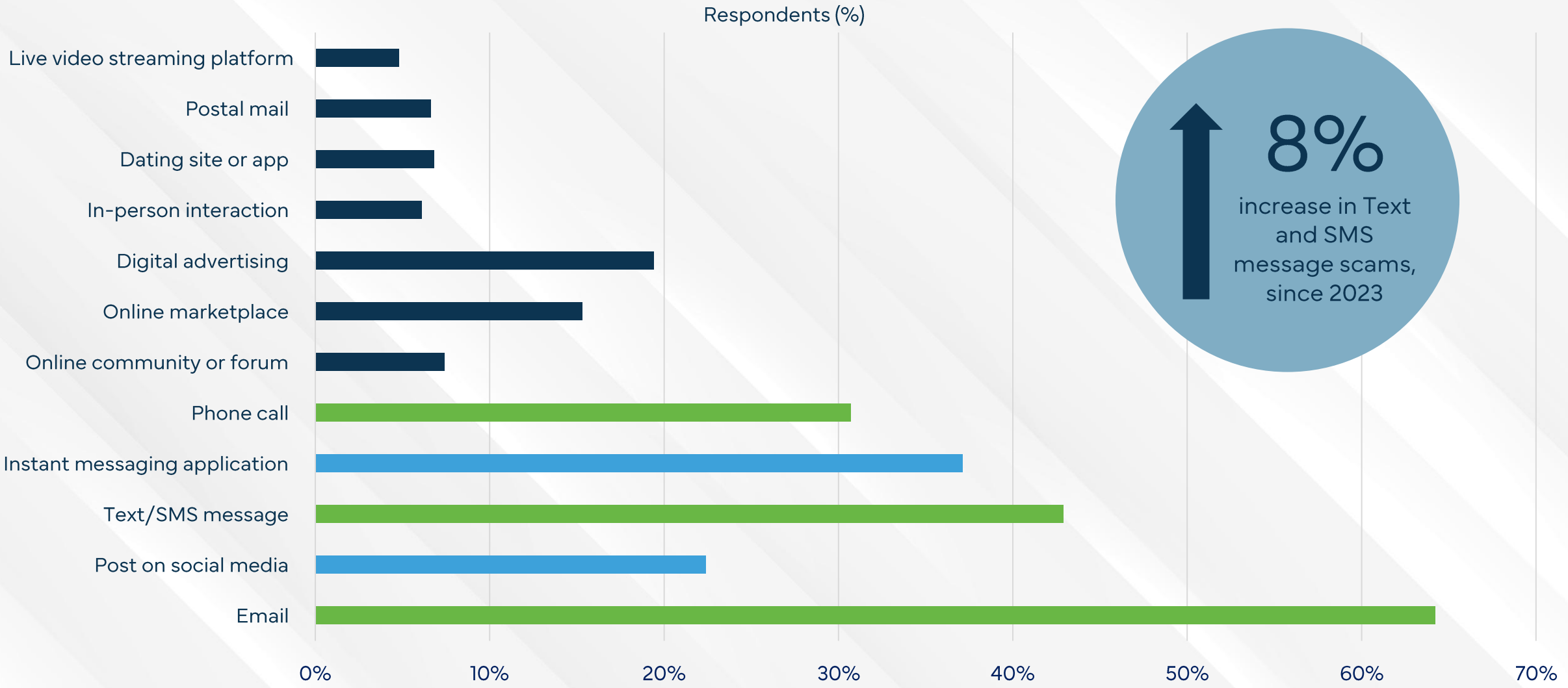
Most Dutch are aware scammers can use AI against them



Awareness of AI-generated text & voices is high, with complex AI videos & images marginally less known.

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

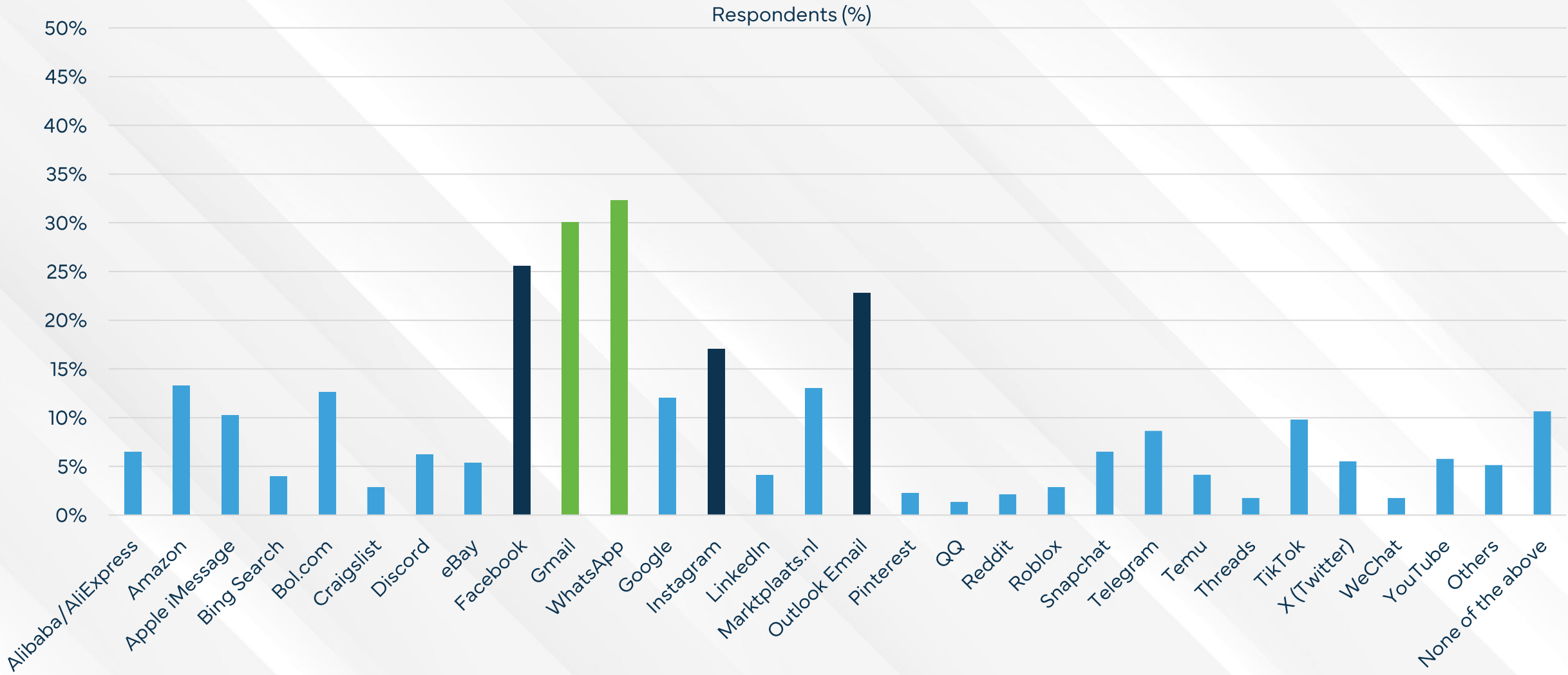
Majority of scams are delivered via Email or Text/SMS Message



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?

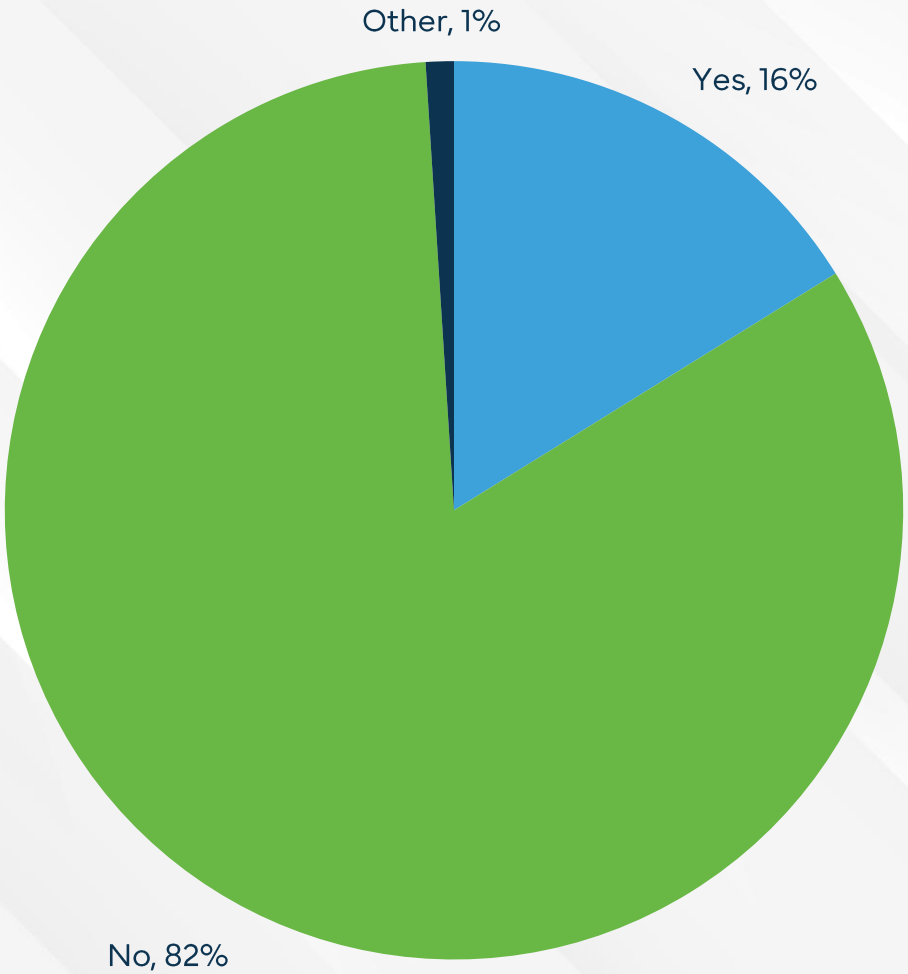
WhatsApp & Gmail are the most popular scam delivery platforms



Facebook, Outlook Email & Instagram make up the top five most popular platforms for scammers.

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

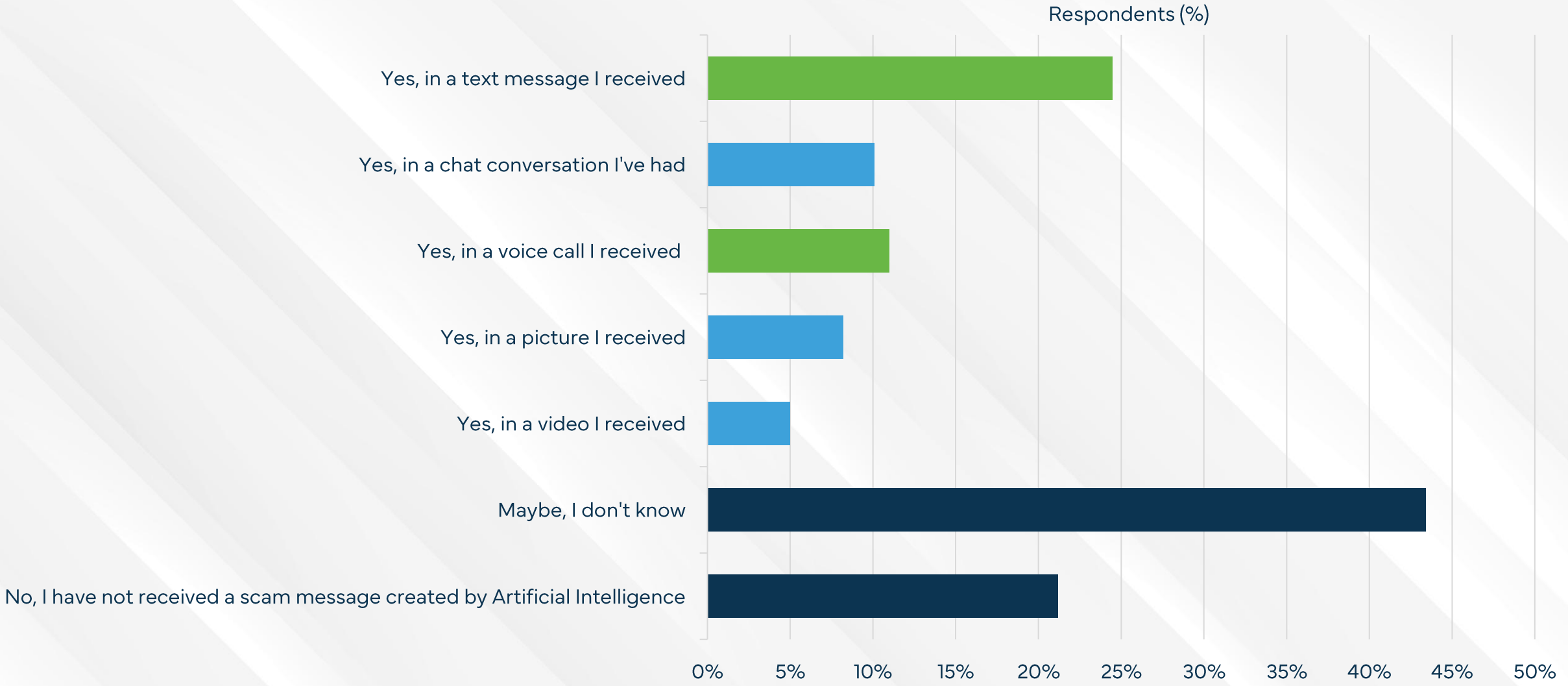
82% of the Dutch did not report the scam to law enforcement



16% 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?

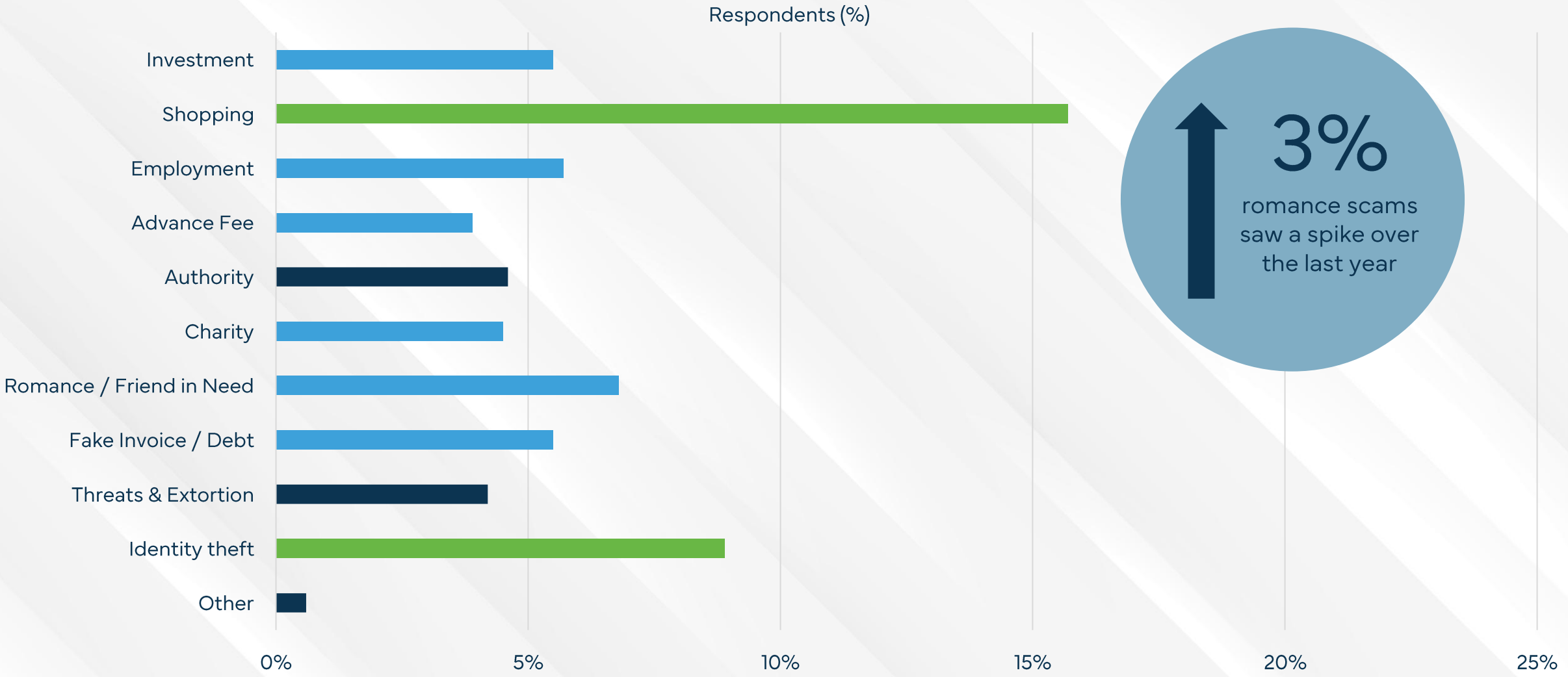
43% were uncertain whether AI was used to scam them



21% of Dutch stated they did not believe they were subjected to scams utilizing AI.

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

Shopping Scams remain the most common scam in Netherlands



3%
romance scams saw a spike over the last year

On average, 0.7 scams were reported per victim, suggesting that scam victims are likely to be retargeted.

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

Hear the stories shared directly from Dutch scam victims

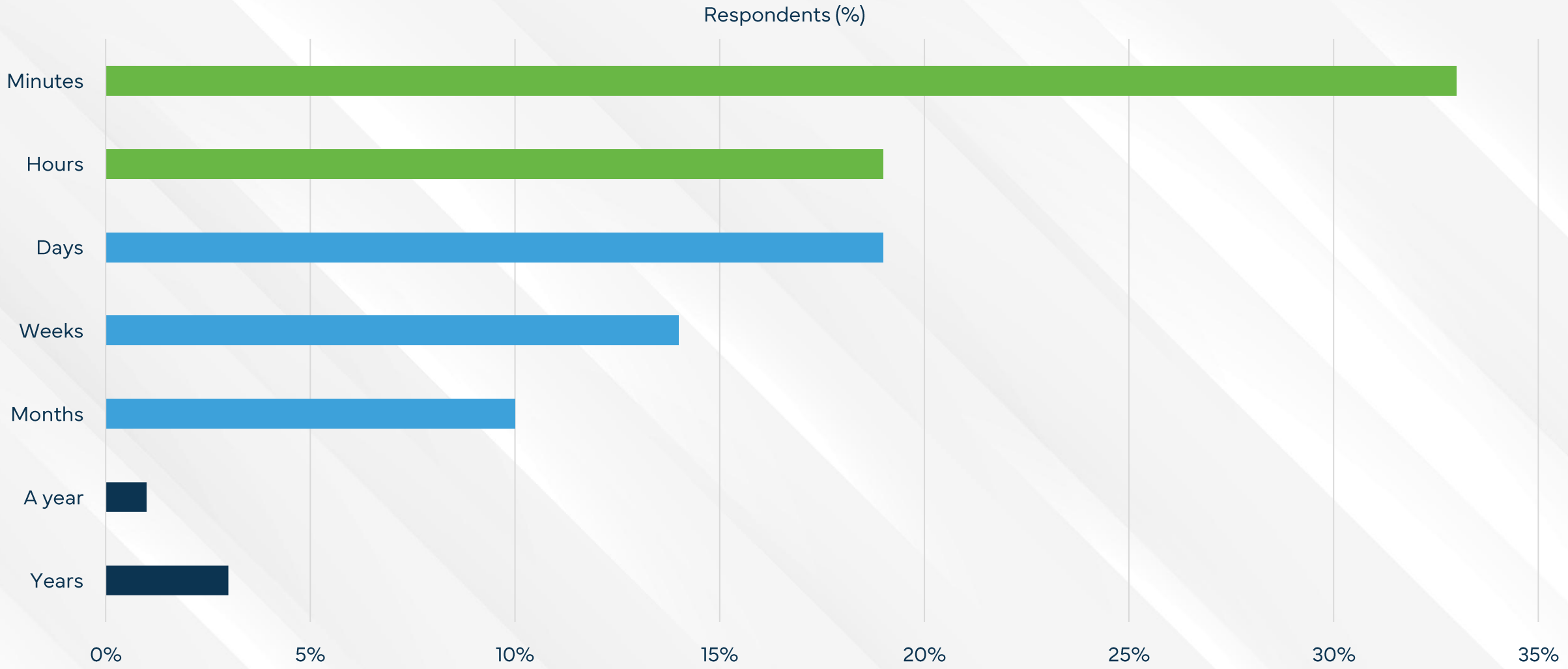
"Well I got an email that my bank card would be blocked but I could prevent that by clicking on a link but when I did that I had to pay 100 euros."

"Invested in something related to bitcoin, so called advertising machines that make your money more valuable. suddenly the site was down and I lost 1000+ euros."

"I received an email from someone claiming to be my housing association saying that I still had to pay my rent even though I had already paid two days before, I called my housing association and told them that I had no outstanding bill, that's when I realized that I was almost scammed."

"I wanted to order a sweater for my boyfriend as a Christmas present. The site looked good and seemed reliable and they had what I was looking for. Ordered here and after a while I got the message that the package was delivered but I had not received anything. After research I saw a lot of bad reviews and it seemed to be a scam. After a long time finally received a cheap sweater from Alibaba but clearly not what I had paid for."

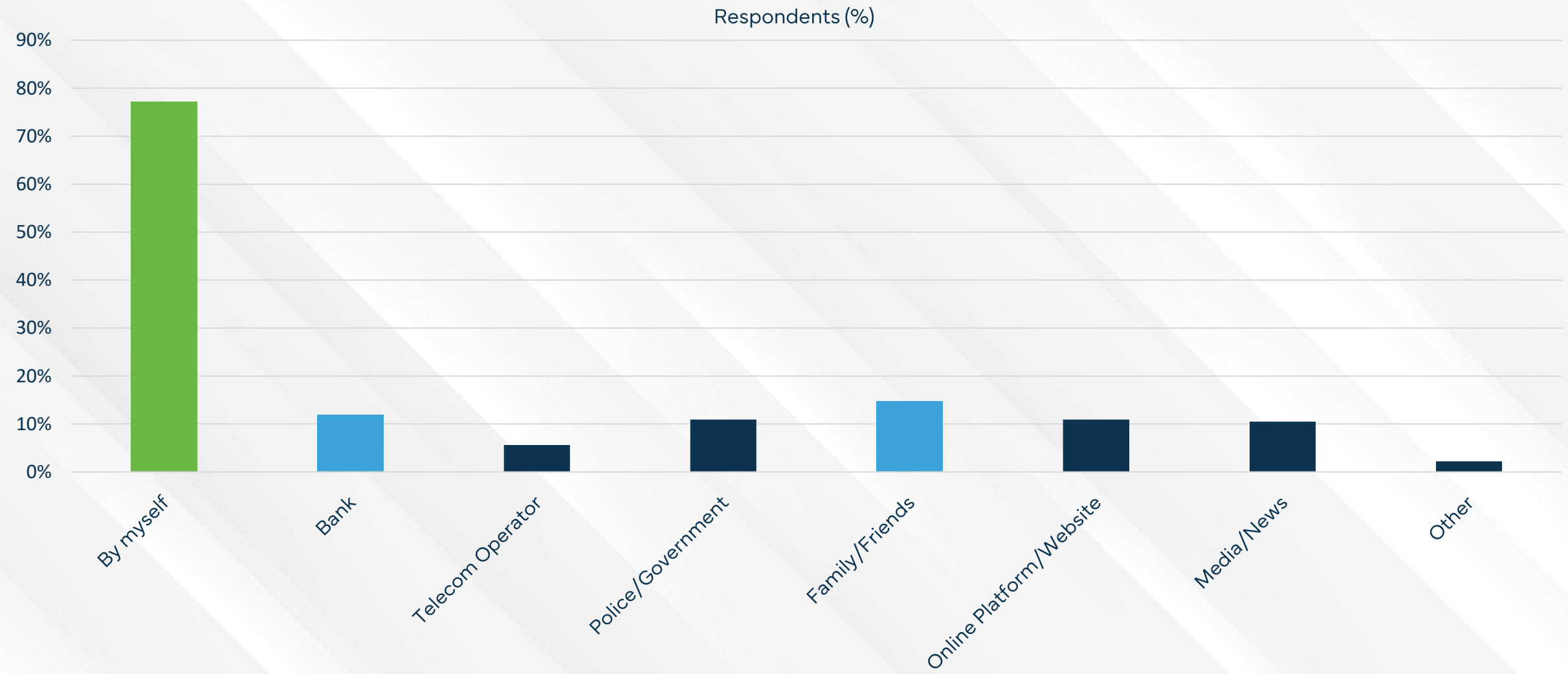
Scammers are swift in the Netherlands completing the fraud within 24 hours of contact



33% were scammed in a matter of minutes, but 4% were targeted with a long con of 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?

77% had to piece together on their own that they'd been scammed

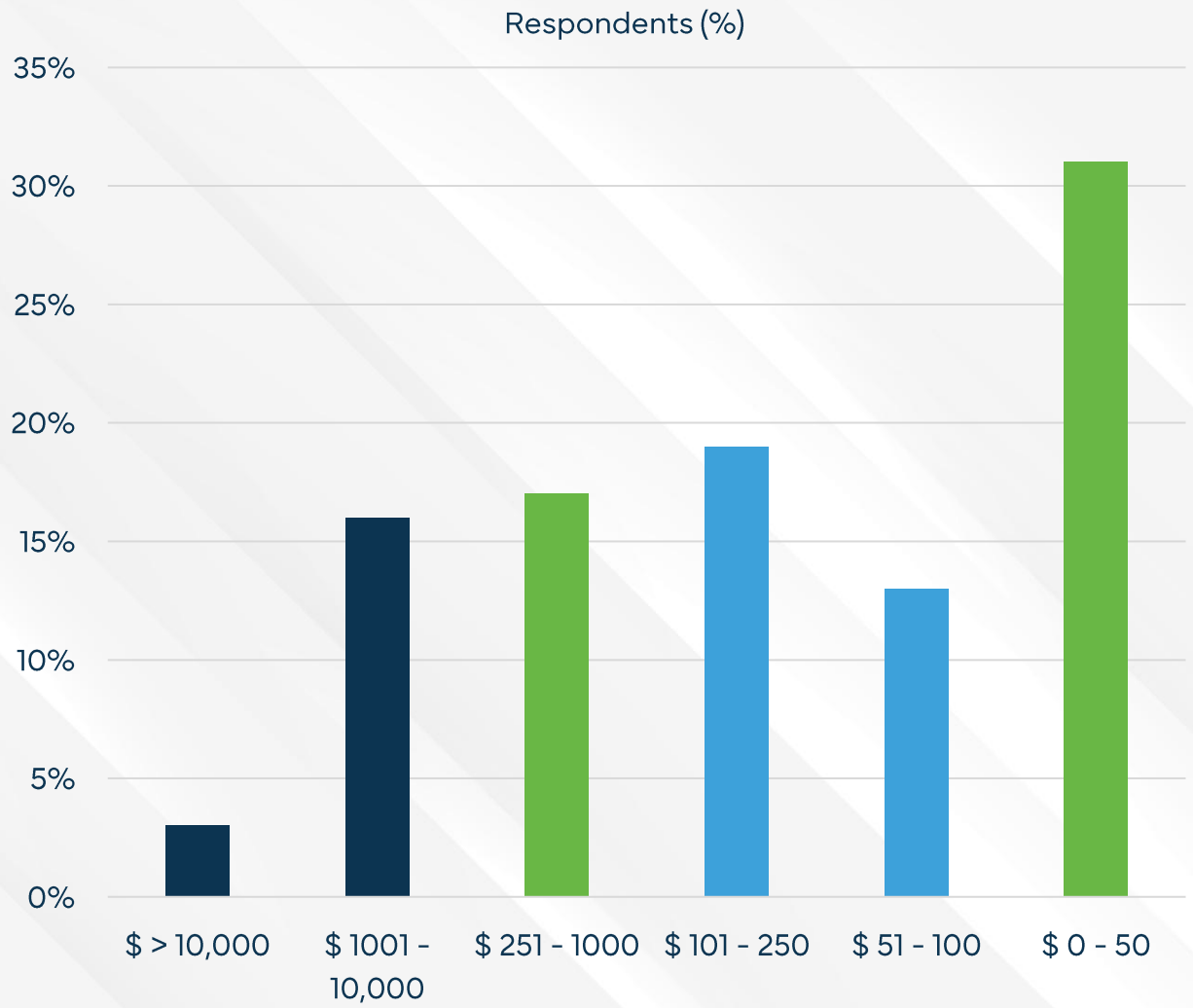


15% were tipped off by friends or family while 1-in-10 were alerted by their banks about the scam.

Q13 - How did you discover you were scammed?

14% of Dutch survey participants lost money to a scam

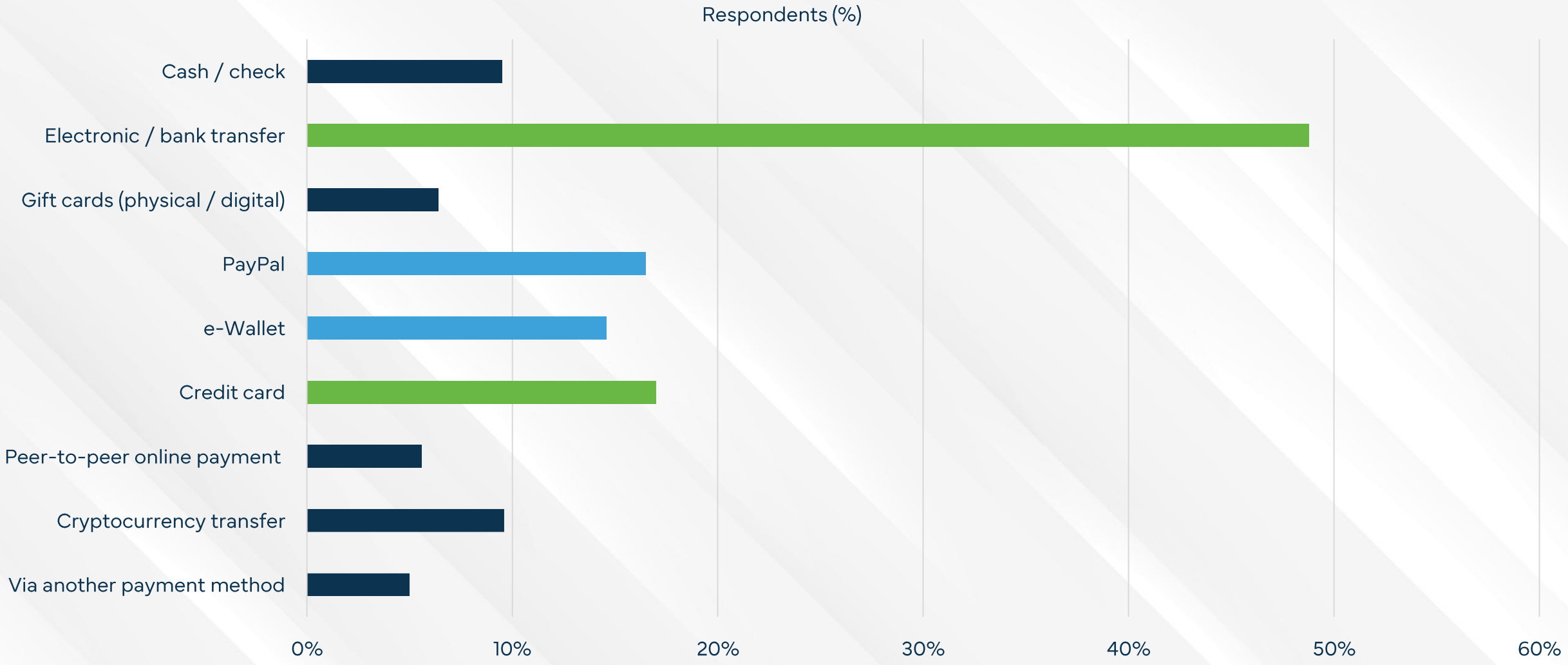
Survey Key Statistics	
Persons approached	1,745
Participants completing the survey	58%
Participants losing money	249
% losing money / approached persons	14%
Average amount lost in US Dollars	938
Total country population	17,772,378
Population over 18 years	14,495,860
# of people scammed > 18 years	2,068,668
Estimated total scam losses (USD)	1,940,410,663
Estimated total scam losses (EUR)	1,750,215,292
Gross Domestic Product (USD, millions)	1,092,748
% of GDP lost in scams	0.2%



In total, Dutch lost an estimated US$1.94 billion to scams, which is equal to 0.2% of Netherlands's GDP.

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

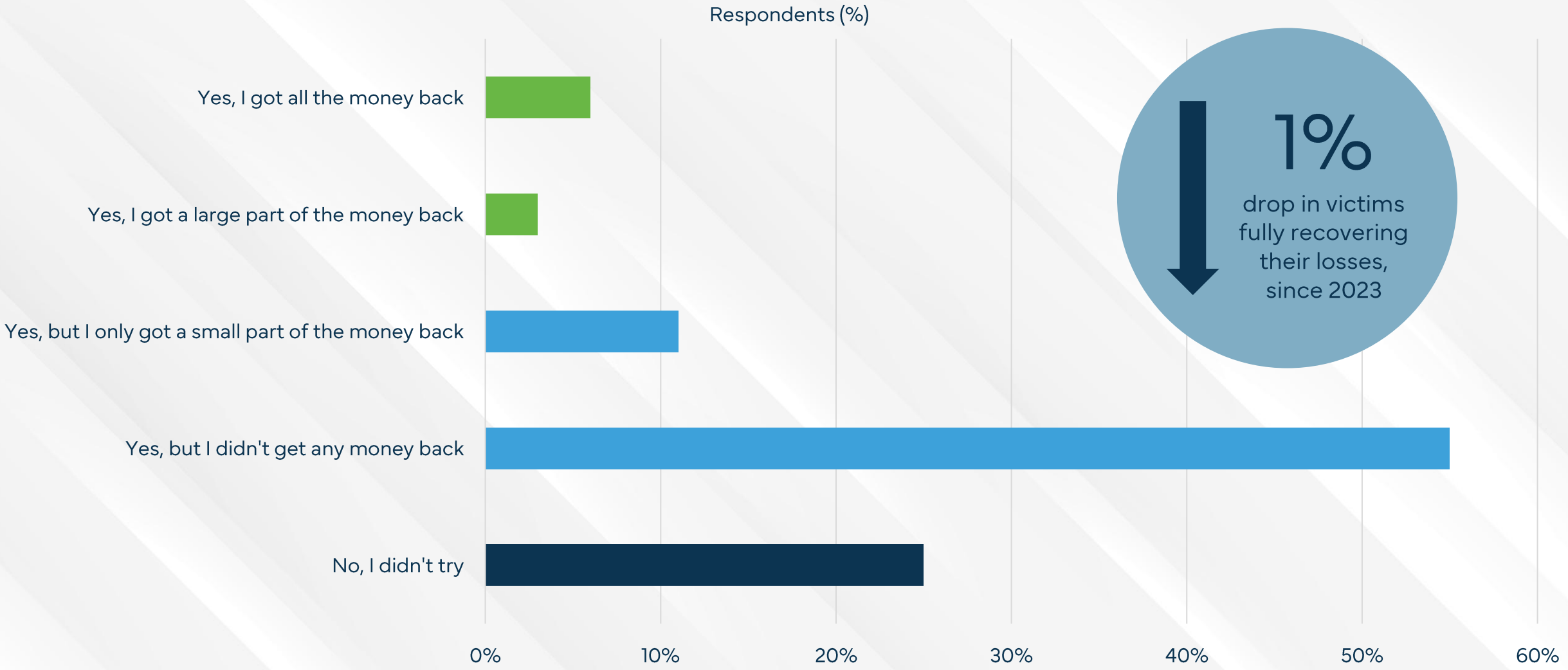
Bank Transfers & Credit Cards are the top scam payment methods



PayPal and e-wallets are also key platforms scammers use to funnel stolen funds

Q15 - How did you pay the scammer?

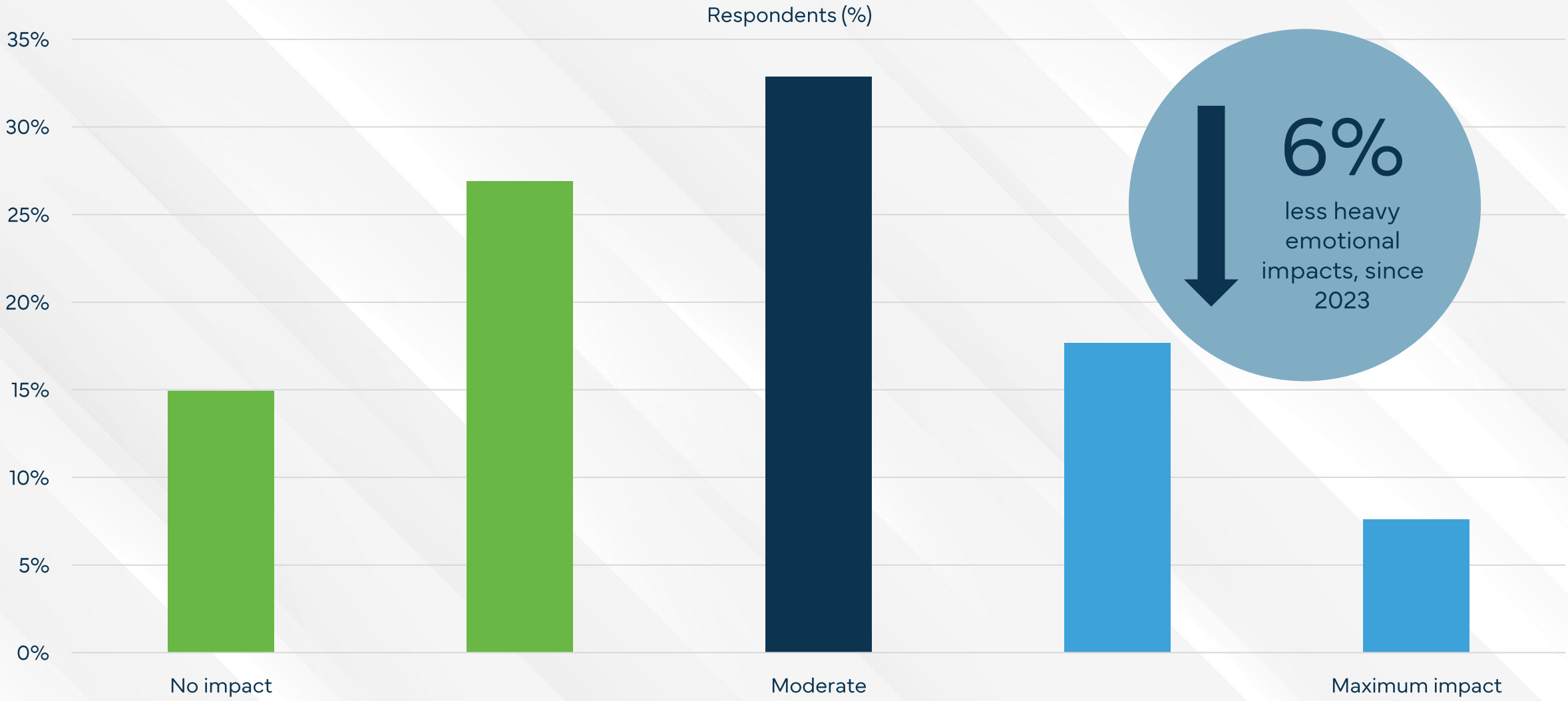
Only 6% of victims were able to fully recover their losses



A quarter did not try to recover their funds. 55% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

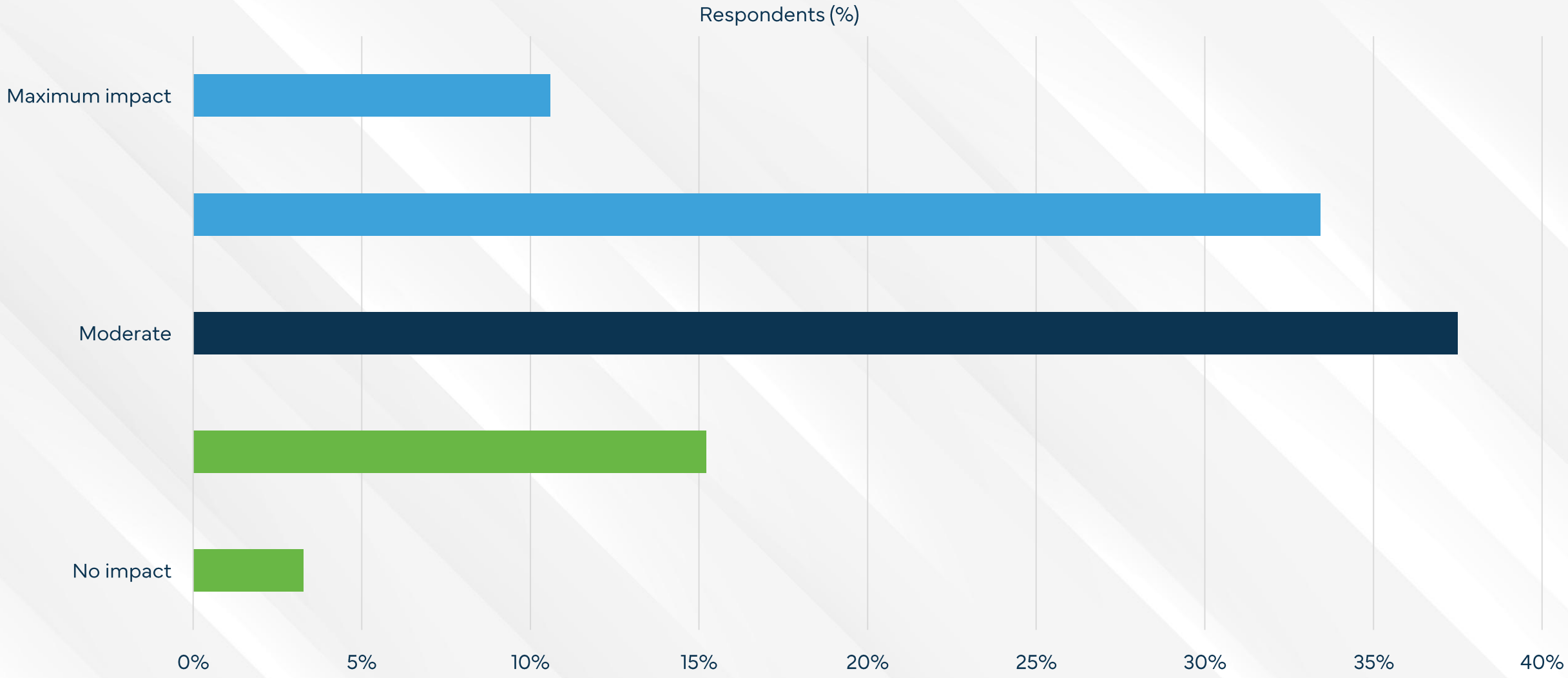
42% of Dutch victims perceived a strong emotional impact



25% of the survey respondents reported little to no emotional impact due to scams.

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

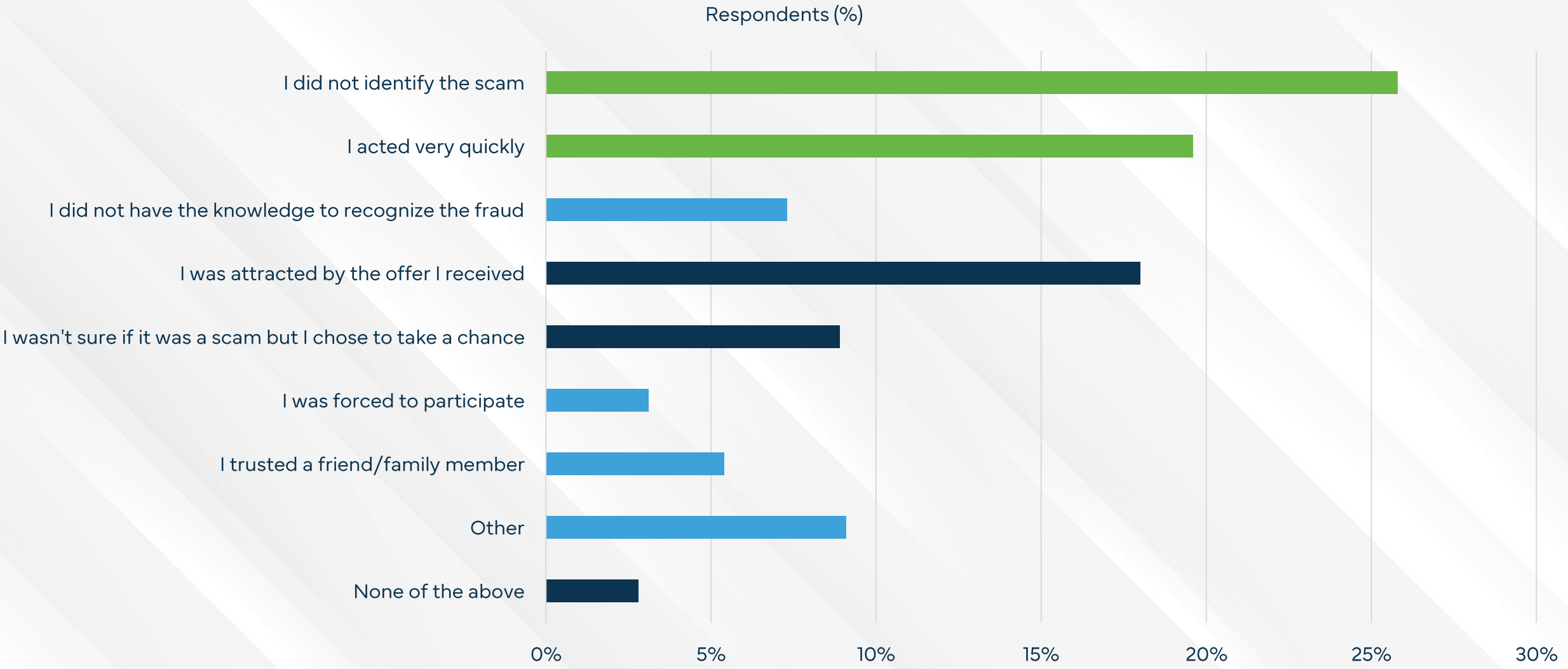
Nearly half of Dutch have less in trust the Internet because of scams



Almost 1-in-5 of the Dutch 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?

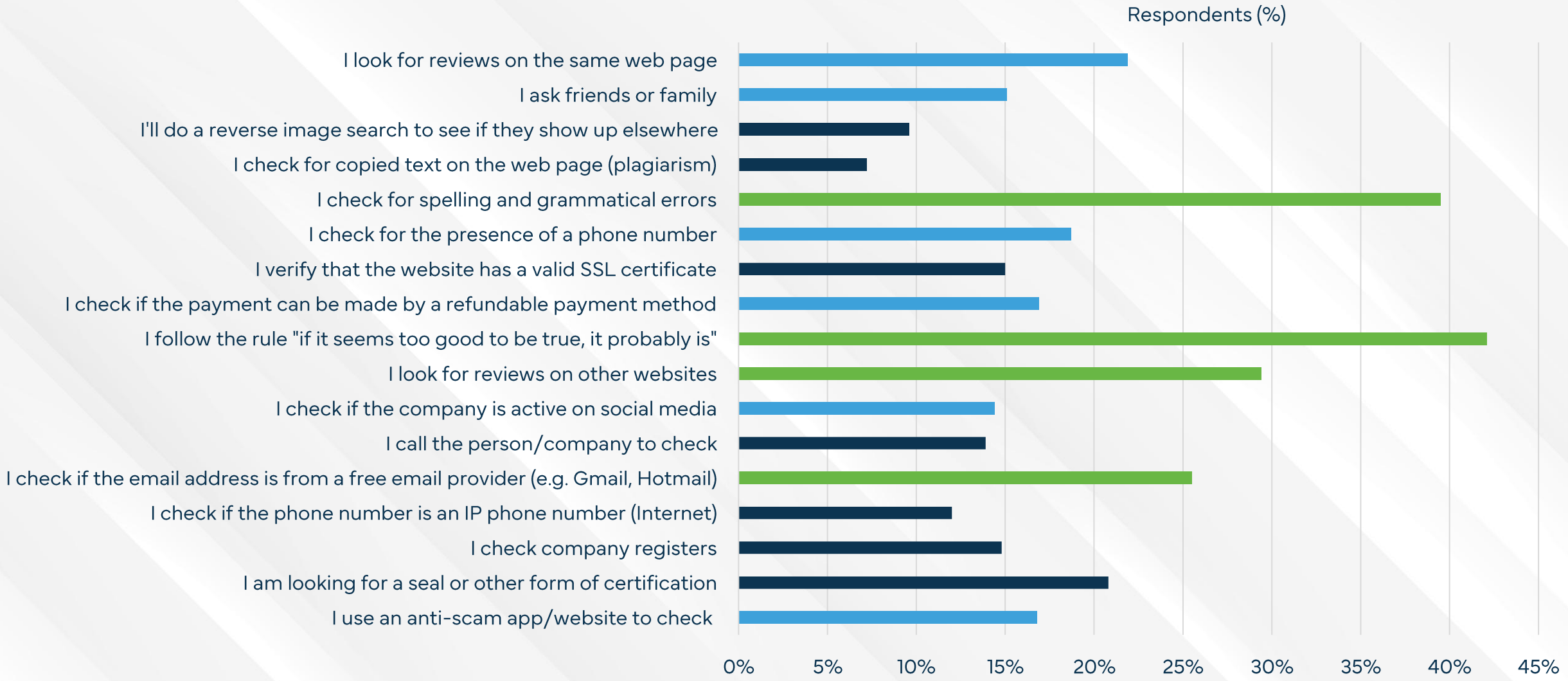
Dutch get caught out by reacting quickly & failing to identify scams



Many fall for the tempting offer, while others gamble despite sensing it might be a scam.

Q19 - What was the main reason you were deceived?

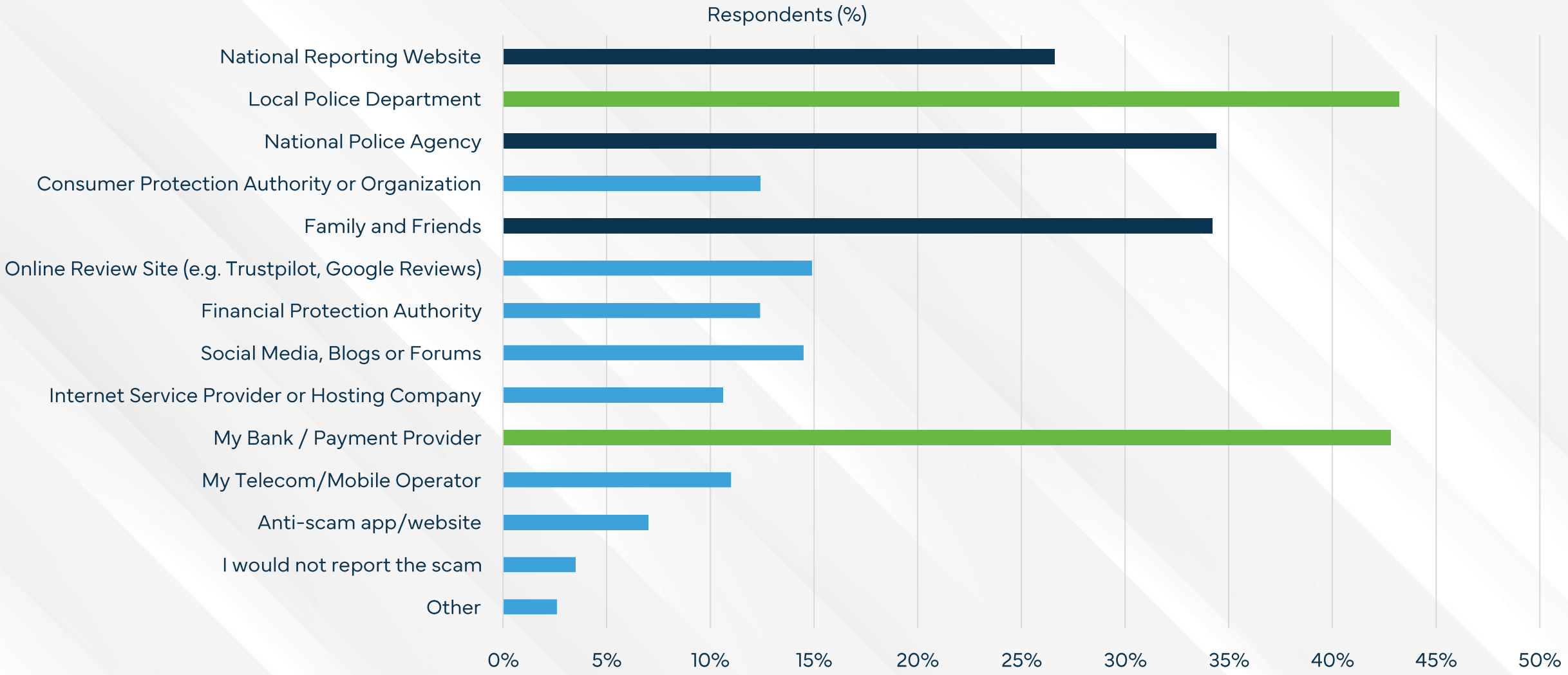
Nearly 1-in-2 Dutch believe “if it is too good to be true, it probably is”



Many respondents rely on checking for typos, grammatical errors, and checking reviews on other sites.

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

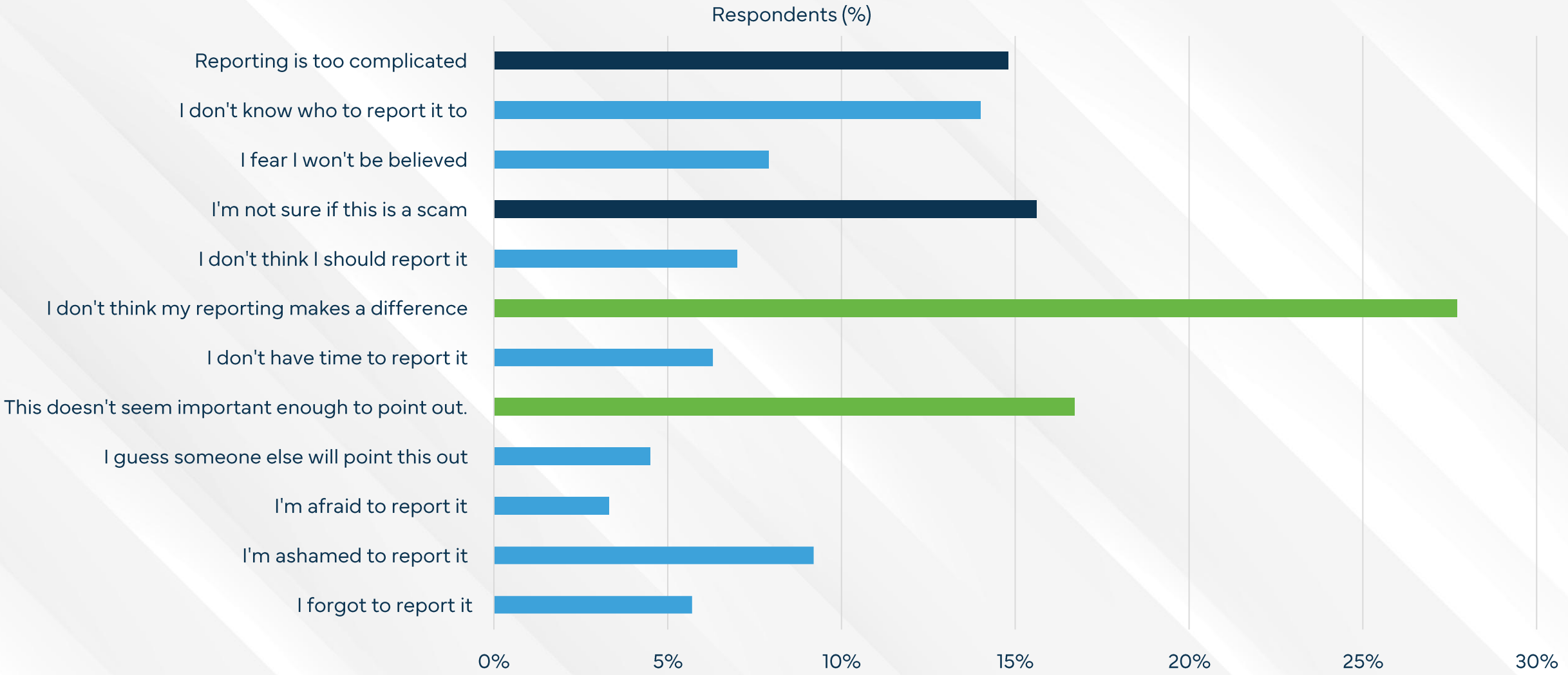
Scams are mostly shared with local police and banks



National police agency, family and friends, & national reporting site are popular places to report scams.

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

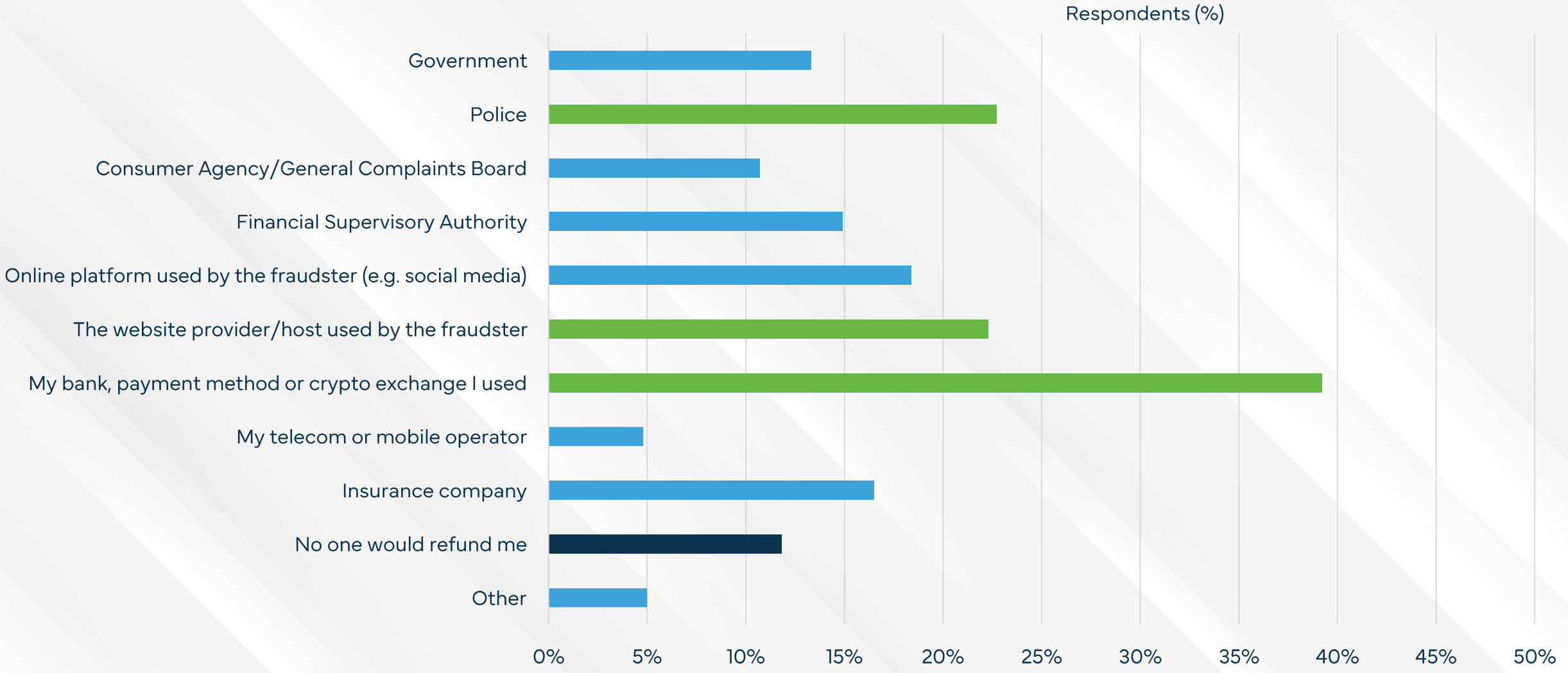
Many Dutch believe that reporting scams won't make a difference



Other do not report scams assuming it's not important enough & uncertainty whether it's a scam.

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

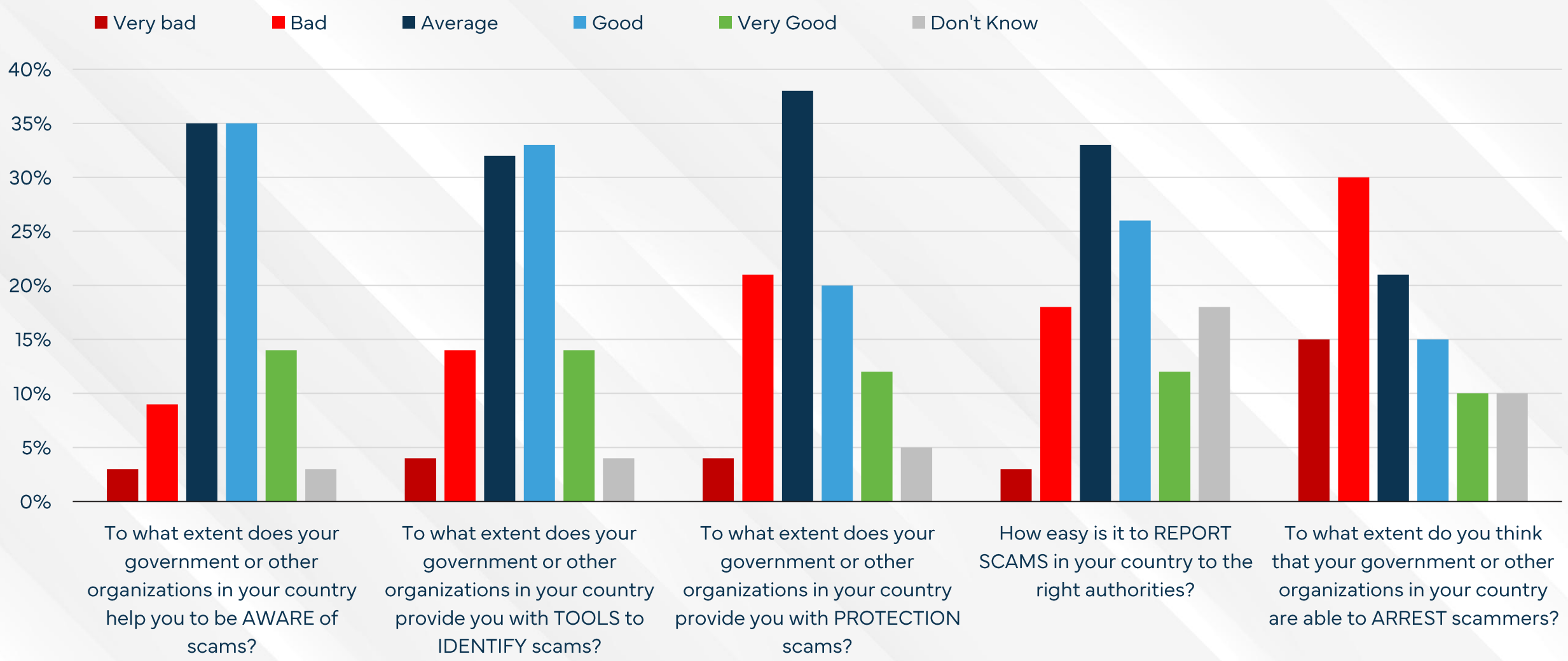
12% of Dutch assume no one will refund their scam losses



Others believe their bank, the police, or the platform used by scammers 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?

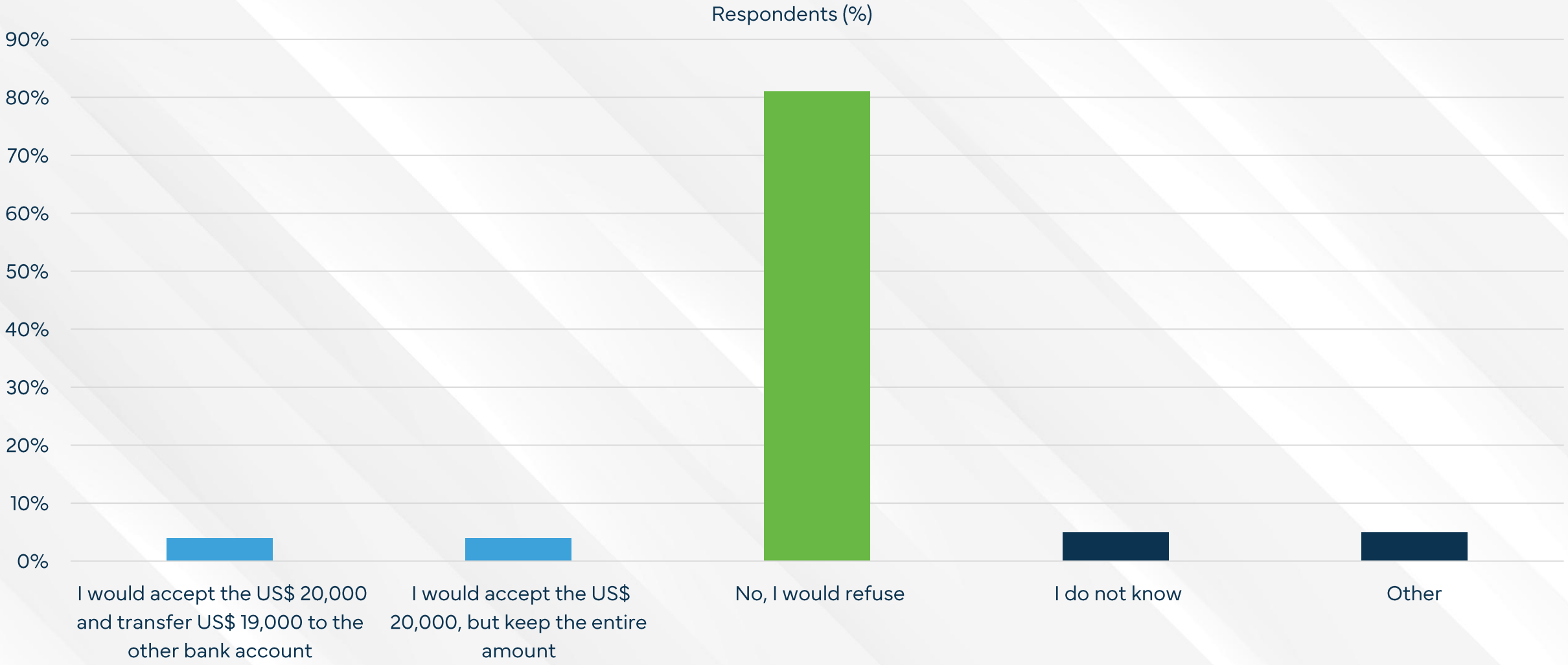
The Dutch public is negative toward their government's efforts to jail scammers



21% of respondents feel the Dutch government's efforts are inadequate, while 47% are content.

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 Dutch admit that they would consider being a money mule



However, 81% of those surveyed claim they 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?

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.

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 contributing 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.

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) supported by 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.

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