BioCatch

The State of Scams in France 2024

GASA
Global Anti-Scam Alliance

Fraudsters target 1-in-10 French as $5.9 billion vanishes in one year

The 2024 State of Scams in France report, an annual study conducted by the Global Anti-Scam Alliance (GASA) and BioCatch, does reveal some shoots of hope, despite a clear disillusionment from the general populace. Through the participation of 2,000 French citizens, we return to the land of liberty to highlight the threats and emerging opportunities for combating those who seek to cheat and defraud the people of France.

Despite growing awareness and improvements in scam recognition, **46% of respondents now report confidence in identifying scams**, a modest 1% increase from the previous year, however this remains below the 2023 world average. The French lack of confidence could work in their favour by promoting a more cautious approach.

Roughly four out of every five participants recalled encountering scams at least once a month, a figure that has risen by 6% since last year and, unfortunately, brings France in line with the global trend. Of those who fell victim to a scam, we discovered a **revictimization rate of 1.85**, with the retargeting of victims becoming increasingly likely in France over the last 12 months.

In the 2023 Global State of Scams report, we found that the most common scams across the world are shopping, identity theft, and investment scams. Together, those scam types account for almost 69% of all scams. In France, however, we see a slight deviation from this global trend. While shopping and identity theft remain the most prevalent threats to the French, citizens are less likely to be targeted by investment scammers. In France, people are far more likely to fall victim to fake invoices and debt collection, or even advanced fee fraud.

The **preferred methods of scam delivery remain rooted in text/SMS messages and emails**, which saw a 19% increase since 2023. The continued use of popular platforms like Gmail and Facebook shows that not enough is being done to counter the strategies employed by fraudsters. They are free to leverage widely trusted channels to conduct their deceitful activities, with Facebook scammers seeing very little resistance to their efforts, while Gmail saw a surge in scam activity.

The emotional and financial repercussions for victims are profound. Only **16% of those scammed were able to fully recover their losses**, and the emotional toll is substantial, with nearly half of scam victims experiencing a heavy emotional impact as a result. The underreporting of scams is a persistent problem, not only in France, with **74% declining to open a case with local law enforcement**. Across the world, the primary reason given for this withering statistic is that people just don't believe anything will be done. This could indicate a deep-seated mistrust in the efficacy of current protective measures and legal recourse, but the other most common answers in France are **a lack of knowledge about who to report to and the perception that reporting processes are prohibitively complex**. Sadly, it seems we have reached an impasse by which the French people let out a collective shrug and ask, "what is the point in trying?"

Despite these challenges, there are signs of progress. The total financial loss due to scams was a heavy **US$5.9 billion (5.14 billion EUR)**. While the number of people losing money to fraud remained stable, France experienced a noticeable reduction in **the average amount lost per person, which plummeted from US$1,464 (1,351 EUR), in 2023, to US$1,107 (1,022 EUR), in 2024**. This is a solemn reminder of the ongoing risks and the need for enhanced preventive measures. US$5.9 billion is an astounding figure that leaves the people of France stranded with little hope of reimbursement.

In conclusion, the people of France need their government, financial, and law enforcement leaders to step forward and educate them. If a nation is resigned to losing their money for good because they believe nothing will happen, they don't know how to pursue justice, or get hindered by an endlessly bureaucratic system, then we have already let them down. Our hope for 2025 is that public education and awareness initiatives are launched to spread the word.

Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

The State of Banking Fraud in France 2024: An In-Depth Analysis

In 2024, banking fraud in France caused colossal financial losses, reaching 5.9 billion dollars, or 0.2% of GDP. This figure illustrates the scale of the problem and the urgent need to adopt more robust strategies to protect citizens. Despite the banks' efforts, new forms of fraud continue to emerge, requiring a more targeted and proactive response.

Massive exposure to scams: alarming figures

The report reveals that 79% of French people are confronted with attempted fraud at least once a month. This figure illustrates an almost daily exposure to fraud, showing that these threats are becoming increasingly common. The fact that 74% of victims do not report these incidents is worrying, as it prevents an appropriate response from the authorities and banks. This lack of reporting can be explained by a perception of the complexity of the procedures or a loss of confidence in the effectiveness of current protection systems. To improve the situation, it is crucial to simplify the reporting processes and raise public awareness of the importance of these steps, by strengthening communication between financial institutions and their customers, regulatory bodies and national authorities.

The challenges facing security technologies in the face of deep fakes

Deepfakes - videos generated by artificial intelligence that convincingly mimic real people - represent a serious new threat to banking security systems. Although banks have adopted advanced technologies such as facial recognition with liveness detection, these systems can be circumvented by sophisticated deepfakes. This situation highlights the need for continuous innovation in security technologies, not only to detect but also to anticipate these forms of fraud. The integration of technologies capable of analysing user behaviour in real time offers an additional defence against these threats, by detecting anomalies before they cause irreversible damage.

Economic insecurity and the lure of gain

The report highlights a worrying fact: 4% of French people say they are prepared to become "financial mules" for a quick buck, and almost 5% are undecided. For a financial institution holding around 8 million accounts, this would represent more than 700,000 accounts belonging to people potentially prepared to engage in mule activity in return for payment. A worrying figure... This situation is often exacerbated by economic insecurity, which pushes vulnerable individuals to accept fraudulent offers. Fraudsters exploit these vulnerabilities to recruit mules to carry out illegal transactions, making it even more difficult to detect and prevent these activities. To meet this challenge, it is essential to strengthen prevention strategies, through awareness-raising campaigns targeting the populations most at risk and by improving mechanisms for detecting suspicious events well before any monetary transactions take place.

The limits of fake adviser scams

"Fake bank adviser" scams remain a major problem for financial institutions. These scams are becoming increasingly sophisticated, making it difficult for banks to distinguish a genuine adviser from a fraudster. Although steps have been taken to secure communications, there is still significant room for improvement. The integration of systems capable of detecting behavioural anomalies such as stress levels enhances protection against these frauds, by identifying subtle signals that escape traditional security methods. Stricter verification of advisor identity and increased monitoring of customer-adviser interactions could also help to significantly reduce the impact of these scams.

Emotional and financial repercussions of scams

The consequences of scams are not limited to direct financial loss. Only 16% of victims manage to get their money back, leaving many of them both furious with their bank and with no real quick recourse other than risky and costly legal proceedings. In addition, the report highlights the considerable emotional impact, with almost half of victims reporting a significant psychological impact, including anxiety, shame and loss of confidence. The re-victimisation rate of 1.85 indicates that victims are often targeted repeatedly, compounding their distress. This situation calls for a stronger response from banks, which could offer more psychological support and improve mechanisms for recovering funds for victims, to minimise the impact of these scams. A pioneer in victim protection, the United Kingdom has introduced regulations under its SPR Act requiring banks and other payment service providers to systematically compensate their customers who have fallen victim to scams. The European Commission has also taken up the issue and is beginning to incorporate some of the SPR provisions into its PSD3 programmatic law, which is due to come into force in 2025.

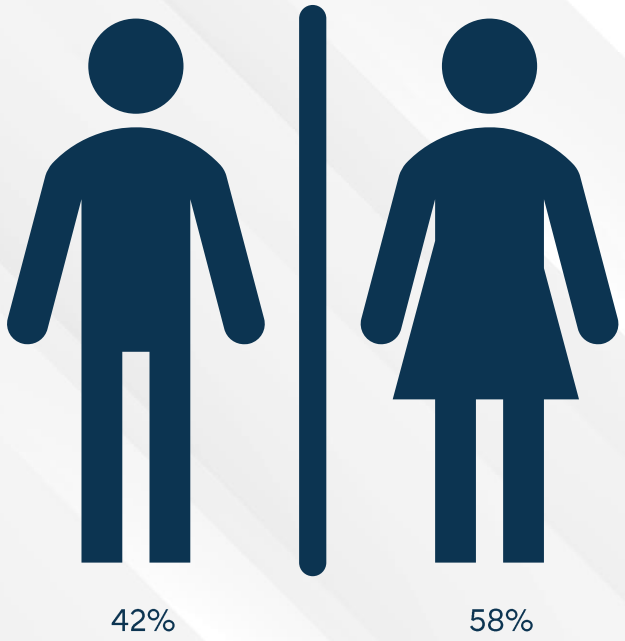
Matthew Platten, CISSP
Solution Consultant - France & Middle East
BioCatch

2,000 French completed the State of Scams in France survey

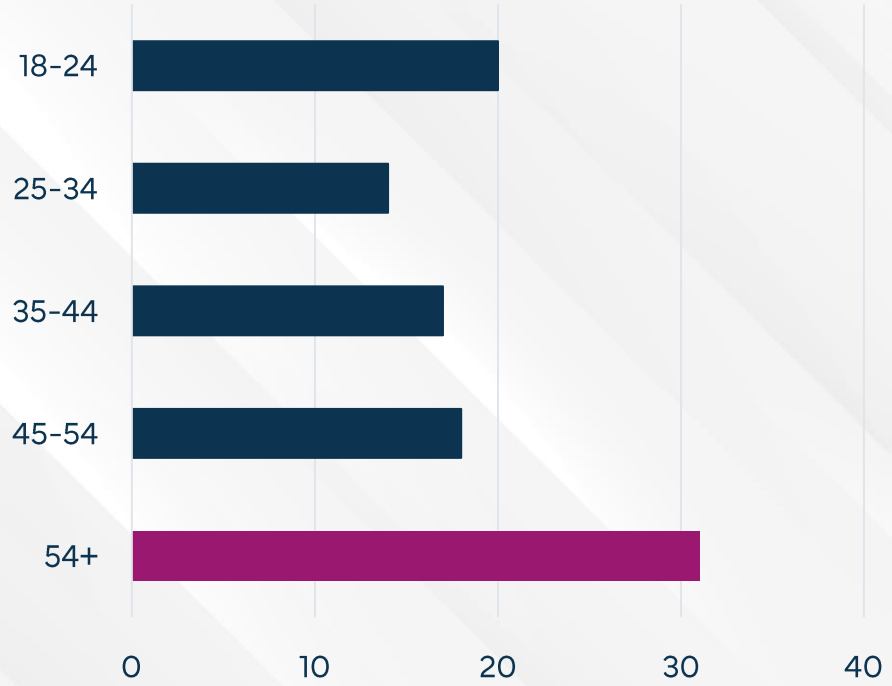
BioCatch

GASA
Global Anti-Scam Alliance

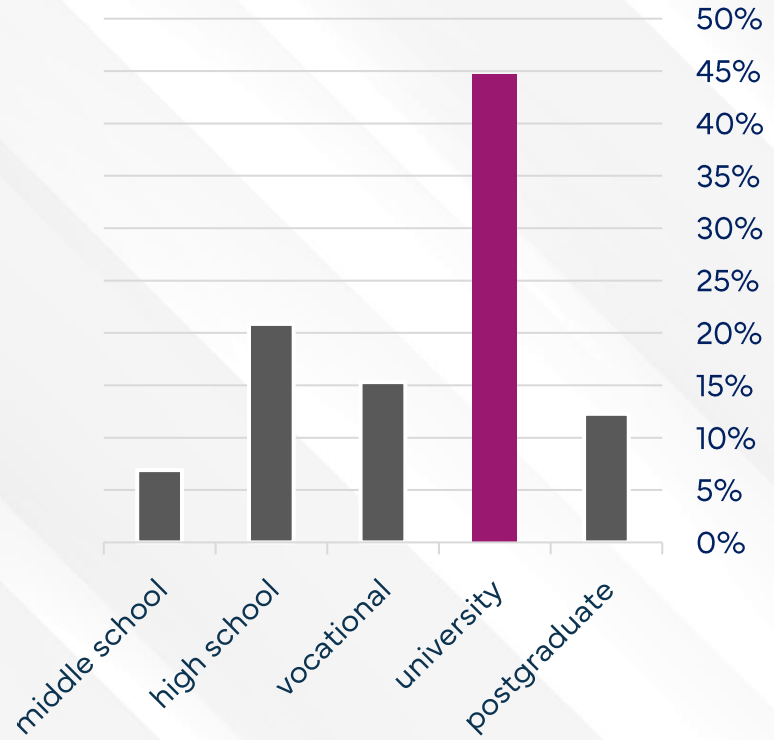
Gender



Age Range

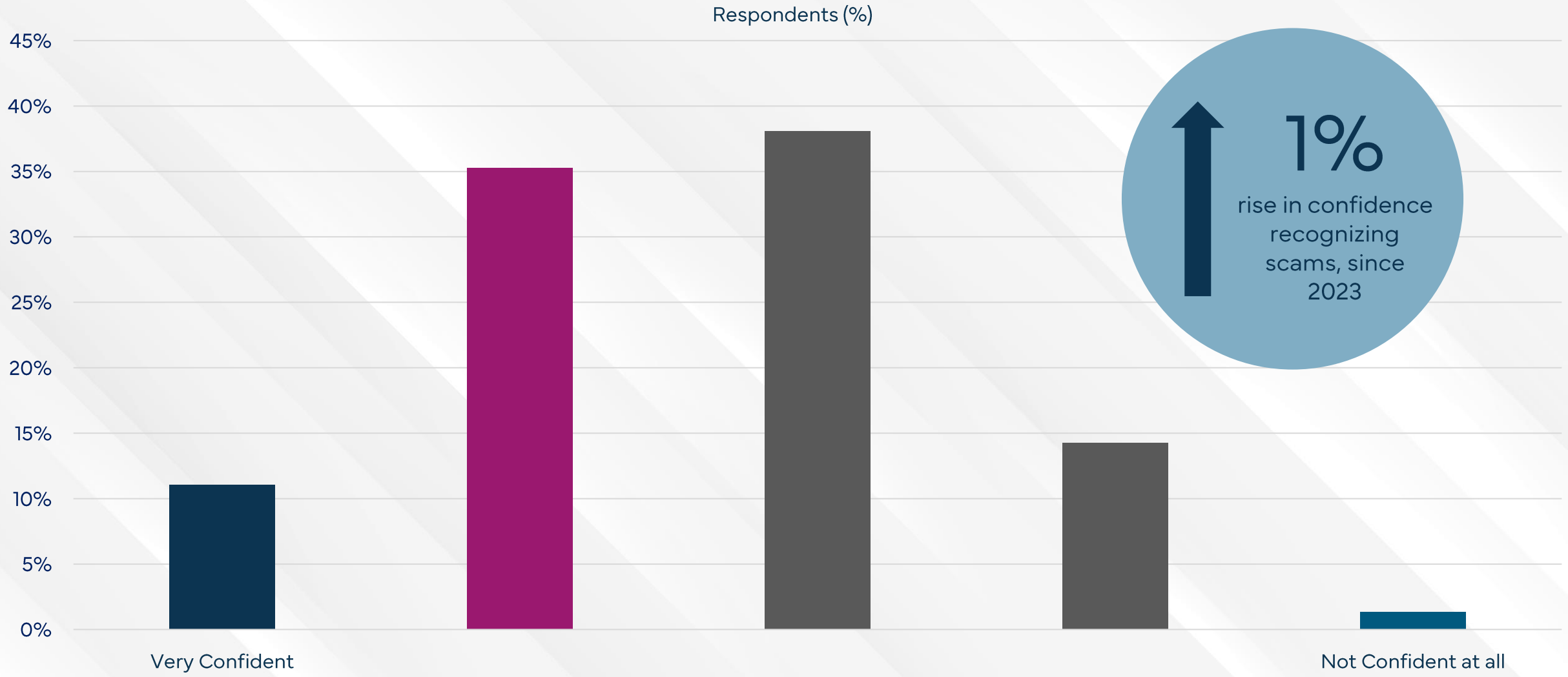


Education



The demography of respondents to the State of Scams in France 2024 survey consists of more women than men. A large proportion were over 54 years of age, with a university degree.

46% of the French are confident in their recognition of scams

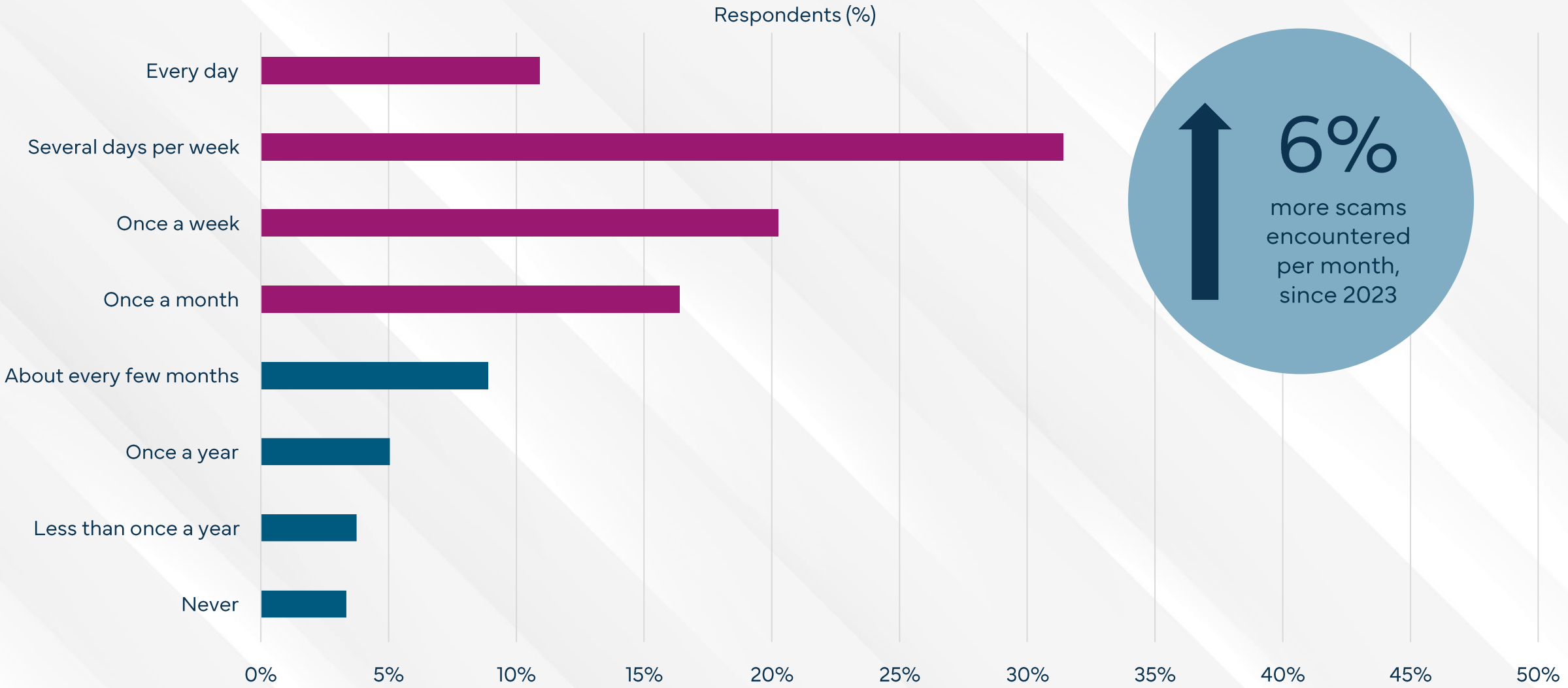


1%
rise in confidence recognizing scams, since 2023

16% of respondents do not trust in their own ability to reliably identify scams.

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

79% of the French encounter scams at least once per month

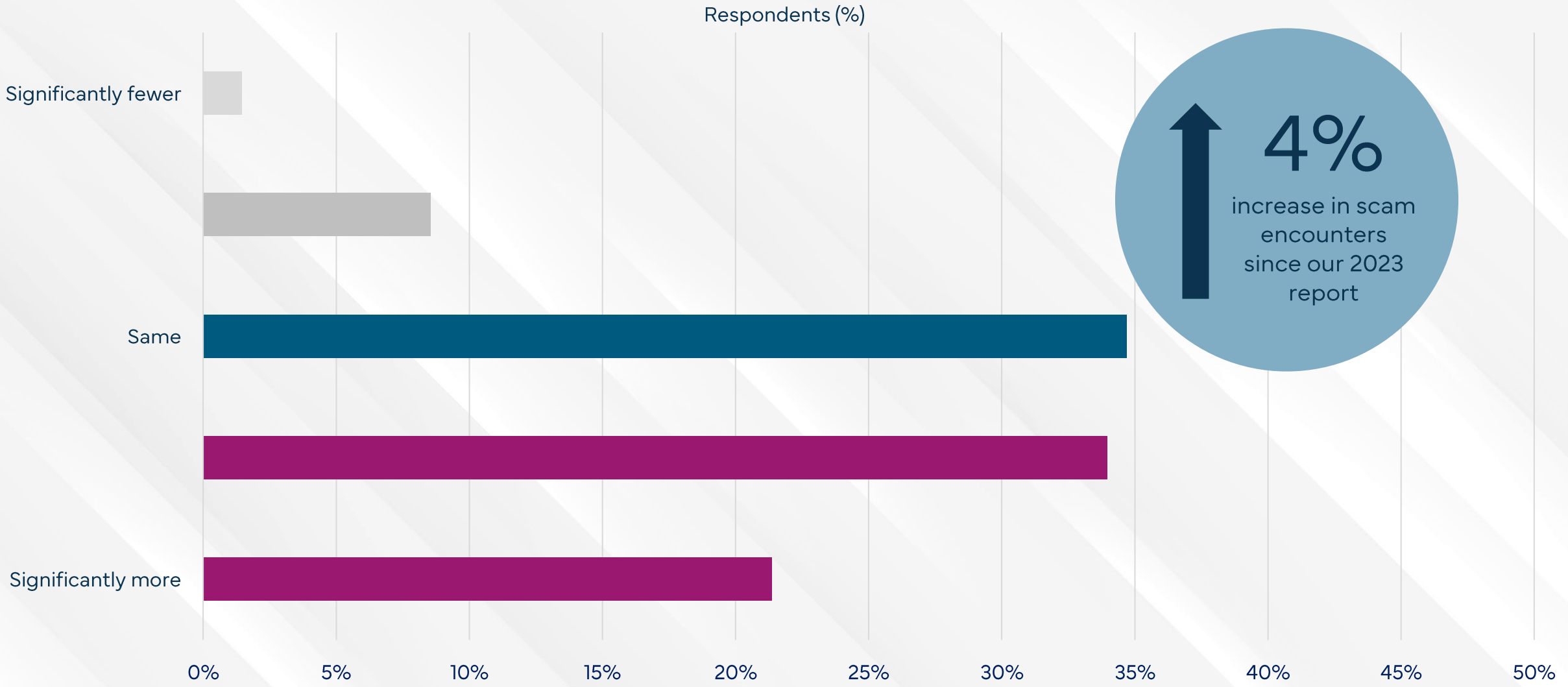


6%
more scams encountered per month, since 2023

Only 12% of French 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.

55% of the French encountered more scams in the last 12 months



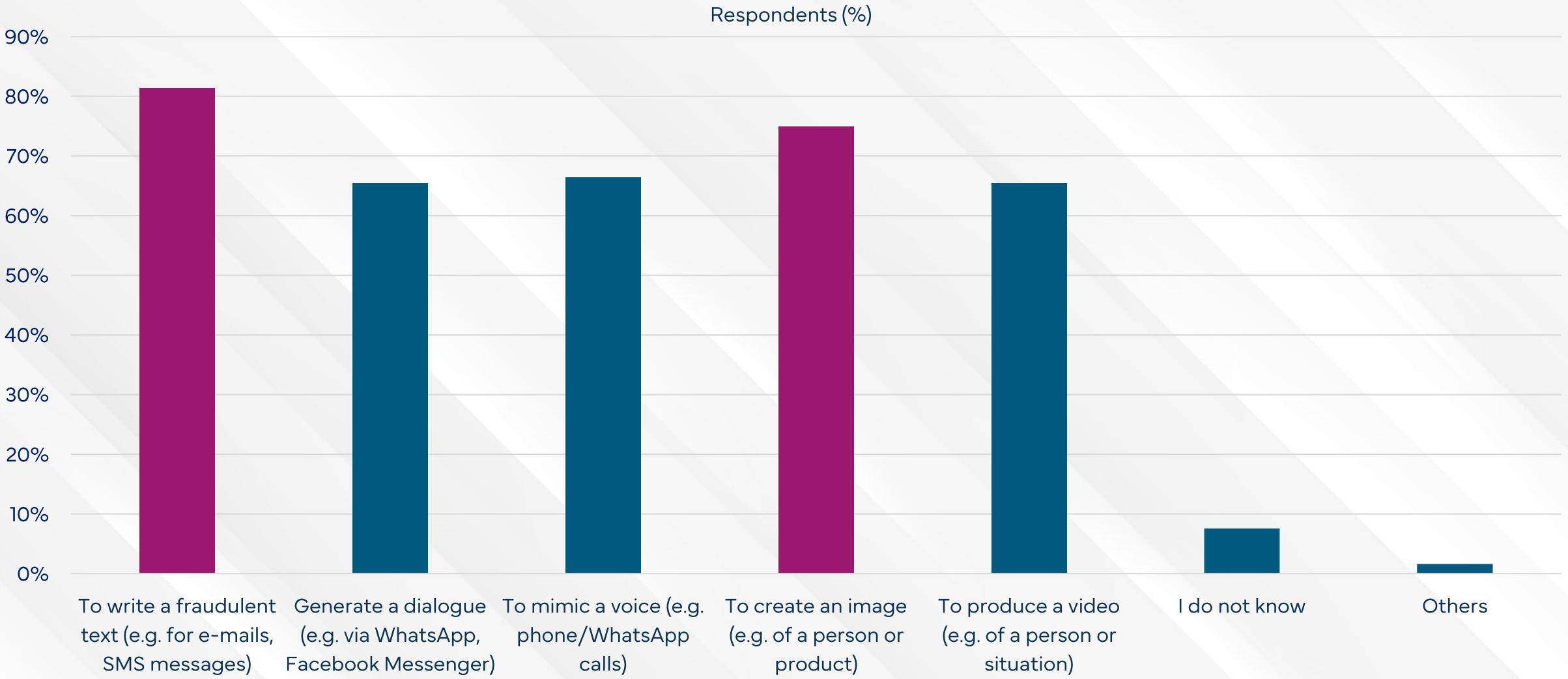
4%

increase in scam encounters since our 2023 report

Only 10% of French 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?

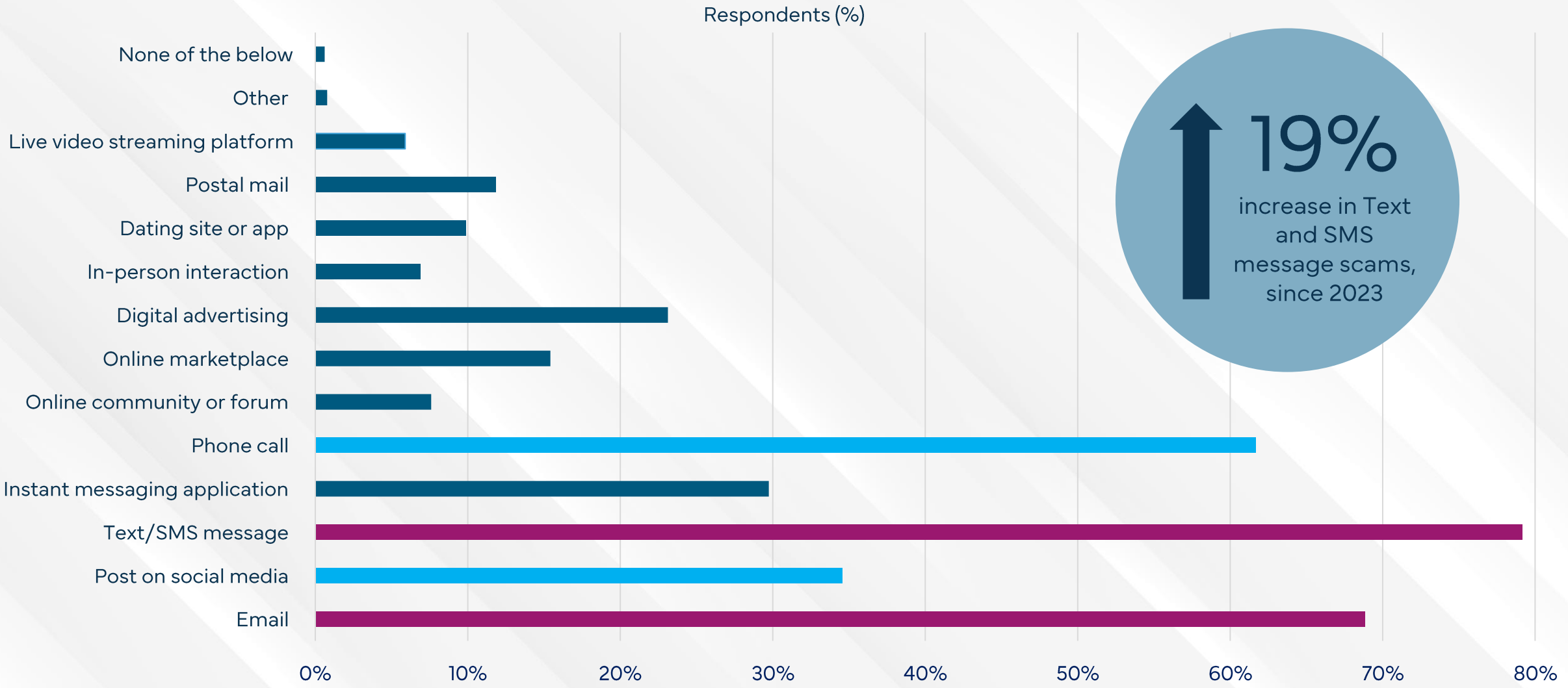
Most French are aware scammers can use AI against them



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

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

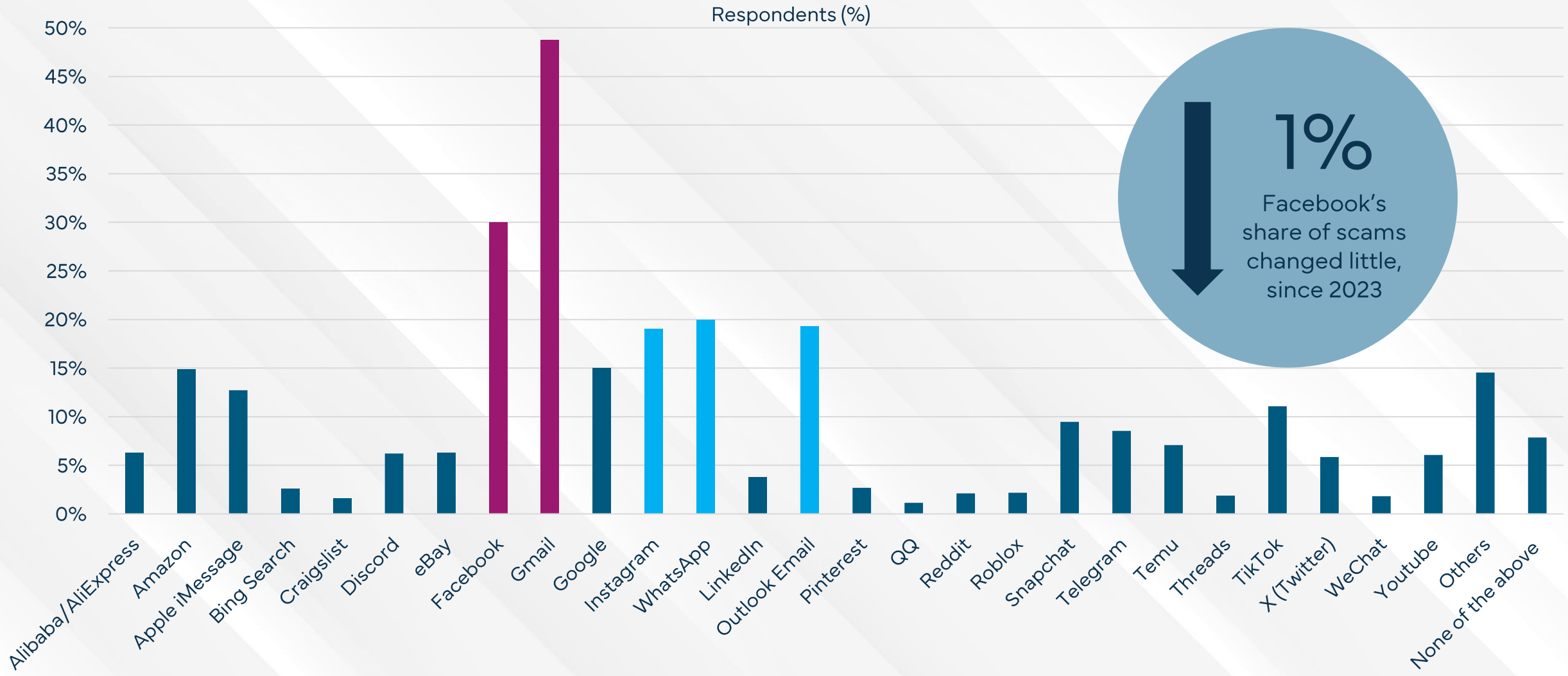
Majority of scams are delivered via Text/SMS Messages or Emails



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?

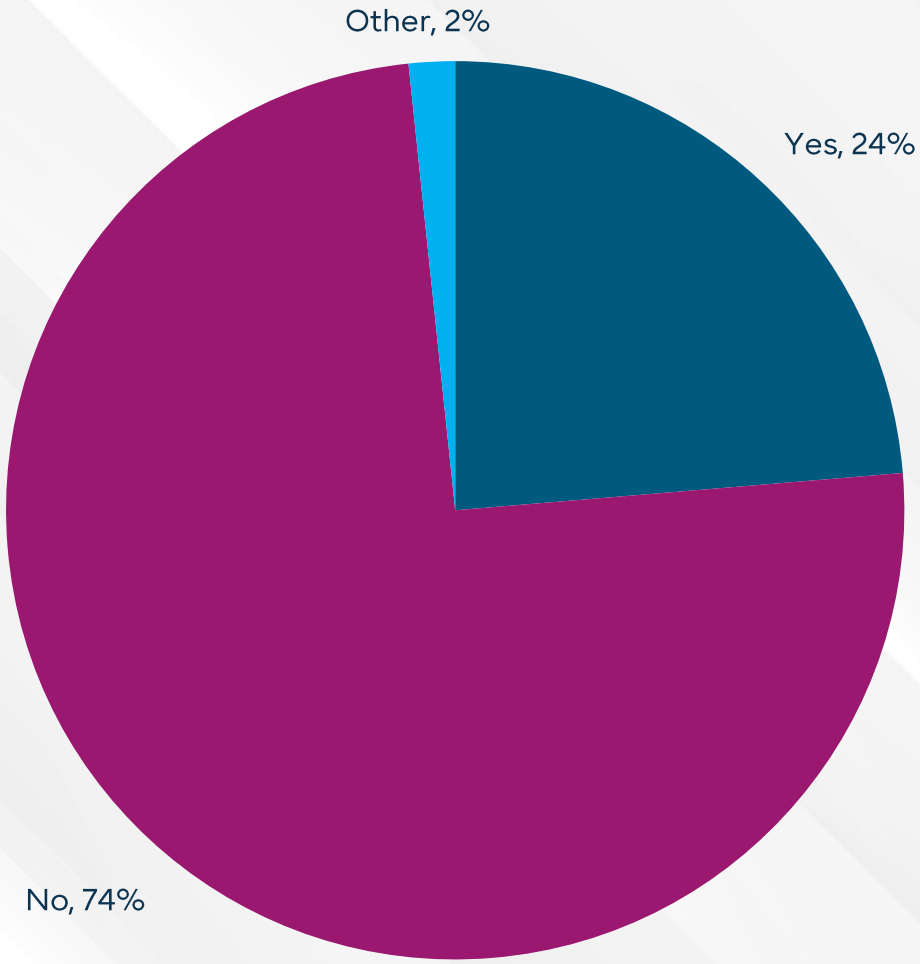
Fraudsters prefer Gmail & Facebook as their scam delivery platform



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

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

74% of the French did not report the scam to law enforcement



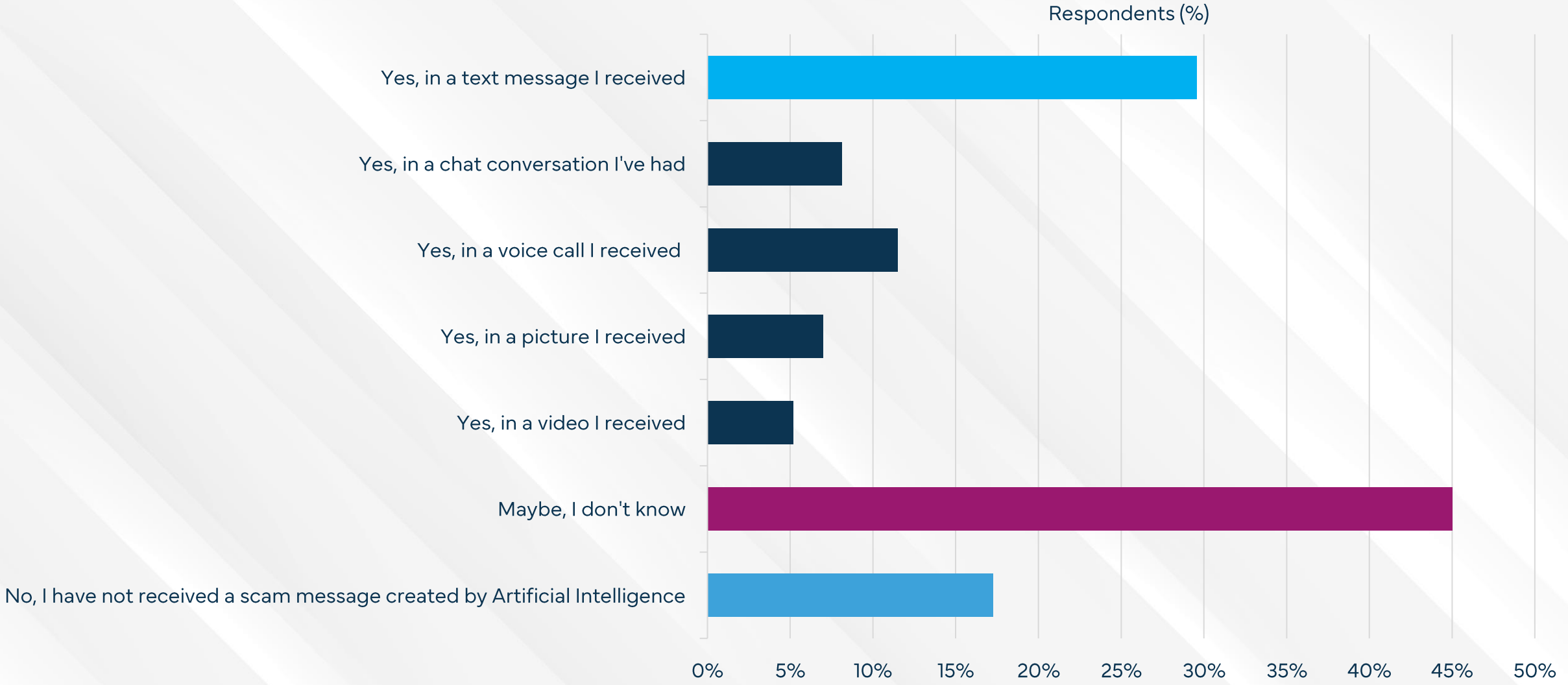
9%

decrease in reports to law enforcement, since 2023

24% 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?

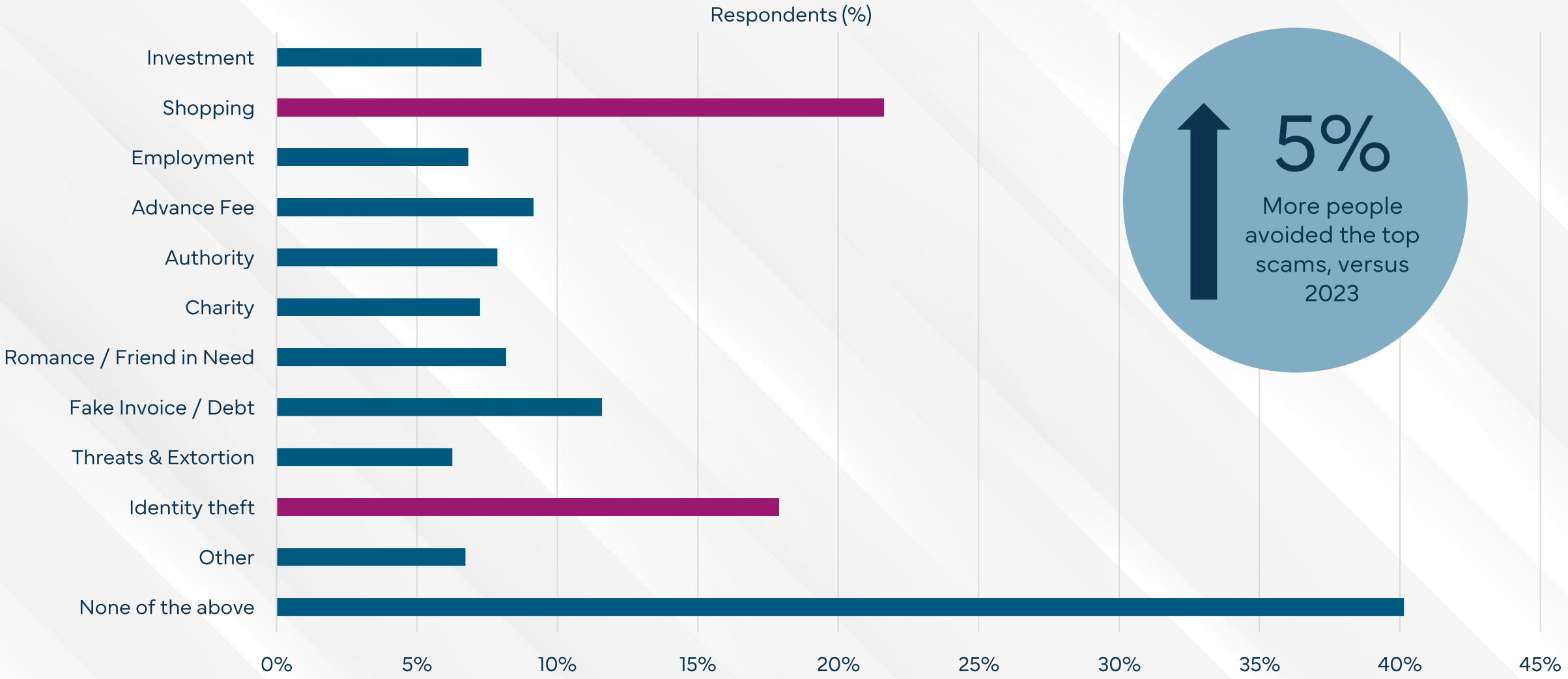
45% of French were uncertain whether AI was used to scam them



17% of the French 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 France



5%

More people avoided the top scams, versus 2023

1.85 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 French scam victims

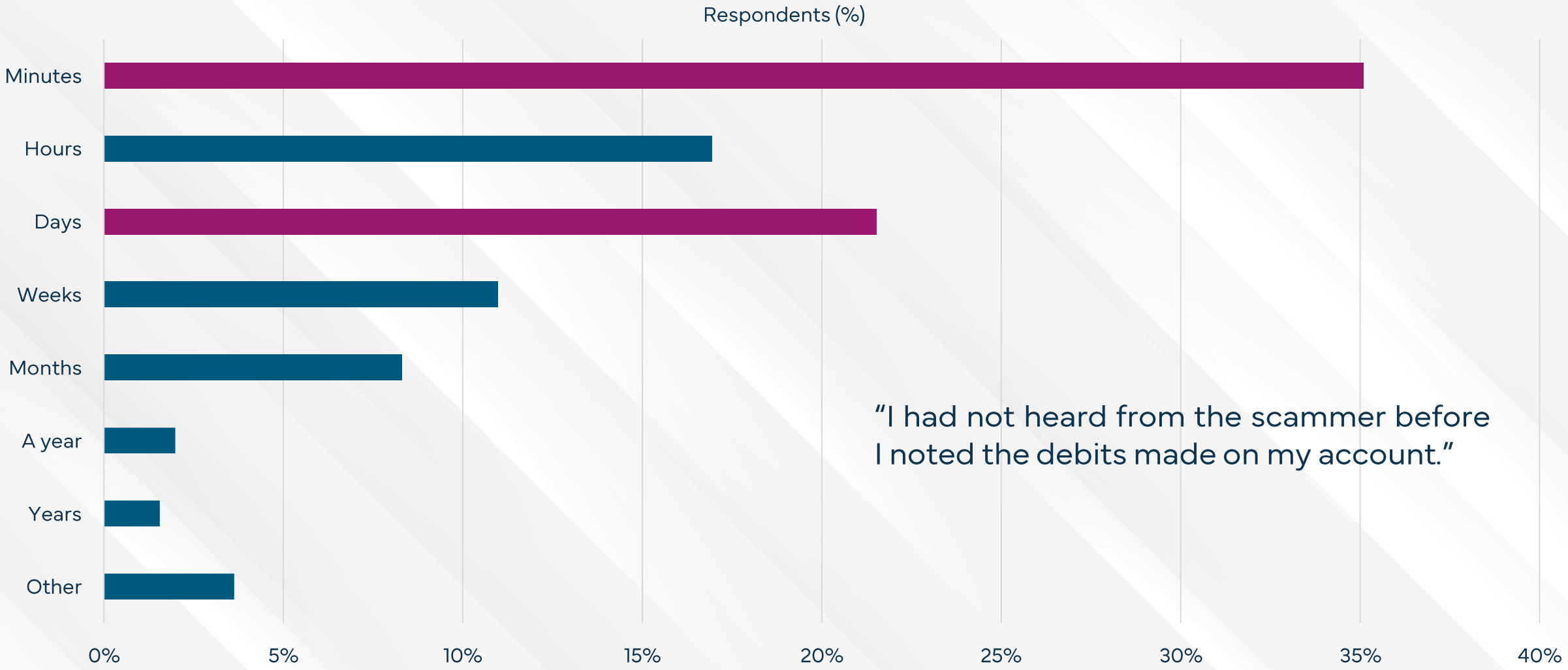
"I got scammed on a fake payment app by entering my bank card. The worst part is that these (scammers) recreated the app very well."

"My computer told me that it had a virus and that I had to call the number listed to resolve the problem, the person on the line asked me for my bank code to troubleshoot ."

"A person pretended to be one of my children asking me to go on (WhatsApp) and give them money for another phone having lost theirs and wanting to buy one right away."

"I responded to a job offer. I had an interview mainly by email then I had the boss's "assistant" on the phone. I needed a machine to carry out my mission and the company sent me a check for the purchase of this machine. I received the check and cashed it. In reality, it was a bounced check. I realized it too late; I had already made the transfer to quickly start my work. I filed a complaint I notified the bank."

52% of scams are completed within 24 hours of first contact

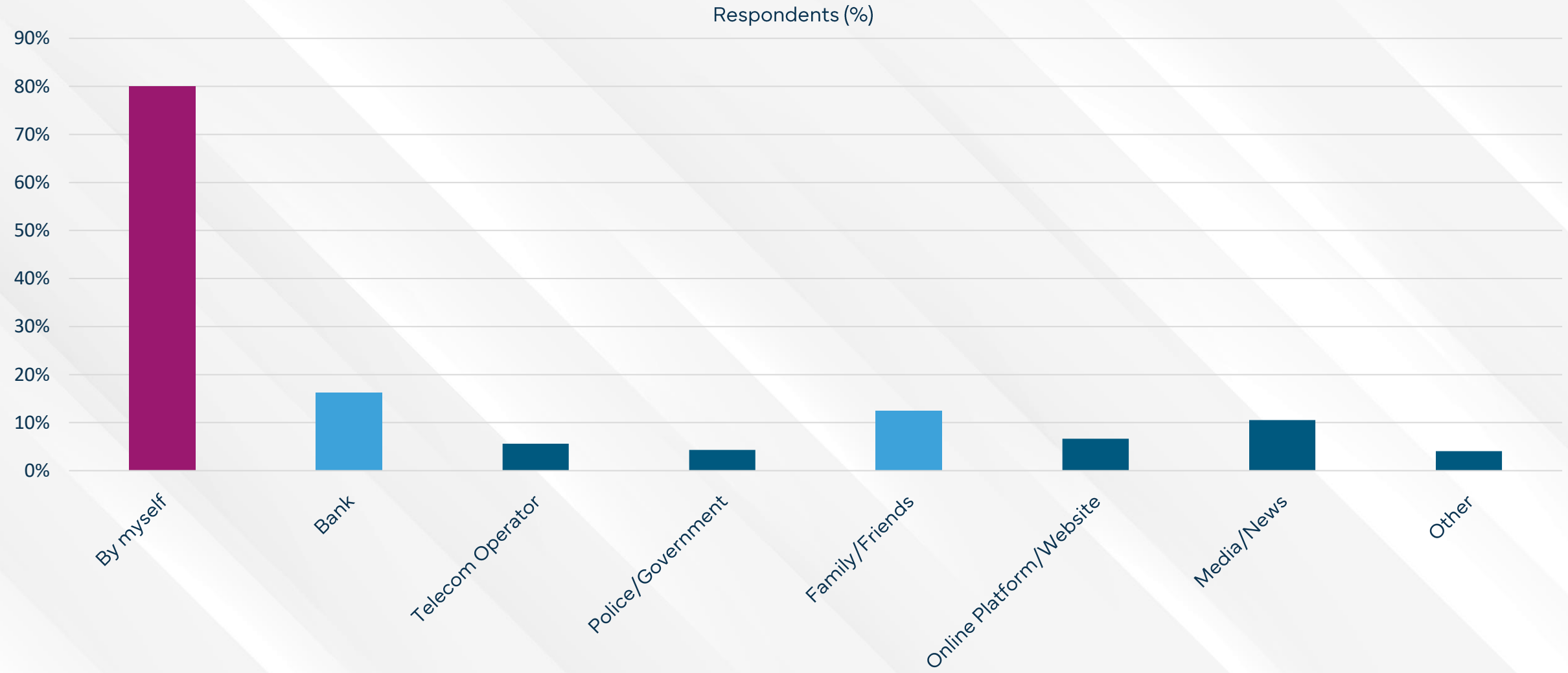


"I had not heard from the scammer before I noted the debits made on my account."

35% 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?

80% came to their own conclusion that they had been scammed

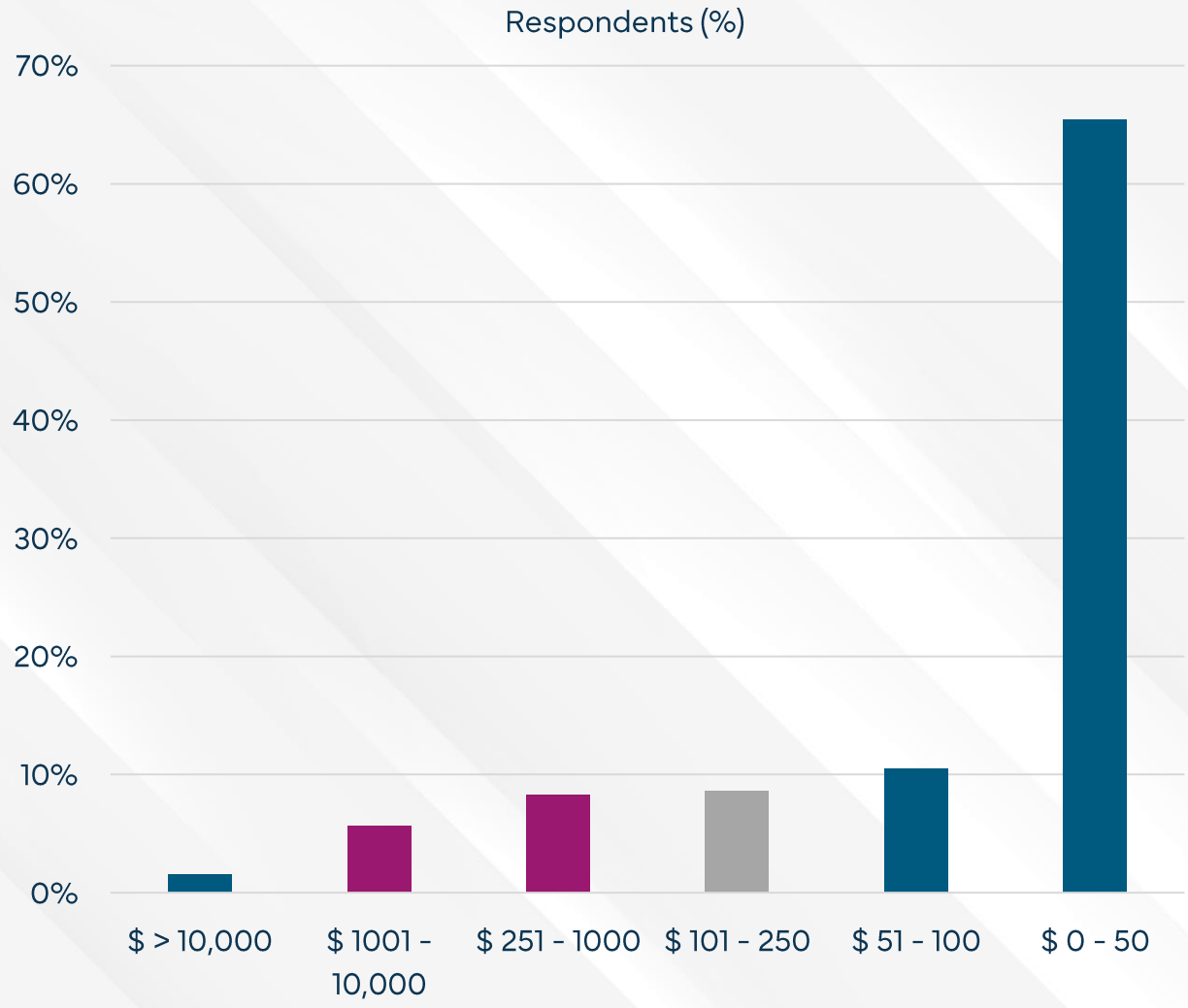


12% were notified by banks, while friends/family are also popular in pointing out scams.

Q13 How did you discover you were scammed?

In total, 10% of French survey participants lost money to a scam

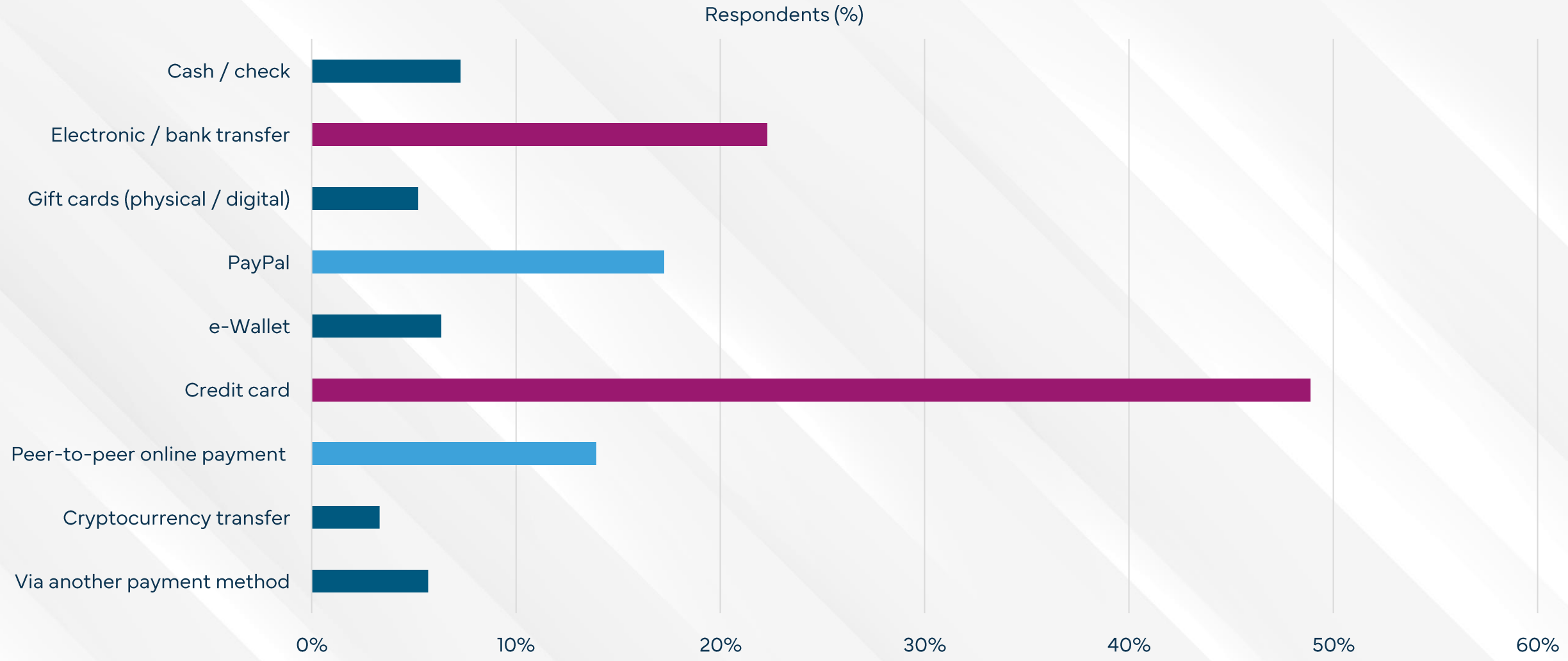
Survey Key Statistics	
Persons approached	6,439
Participants completing the survey	31%
Participants losing money	632
% losing money / approached persons	10%
Average amount lost in US Dollars	2,181
Total country population	68,374,591
Population over 18 years	53,989,039
# of people scammed > 18 years	14,385,552
Total scam losses (USD)	5,854,664,250
Total scam losses (EUR)	5,141,382,878
Gross Domestic Product (USD, millions)	3,049,016
% of GDP lost in scams	0.2%



In total, the French lost $5.9 billion to scams, which is equal to 0.2% of France's GDP.

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

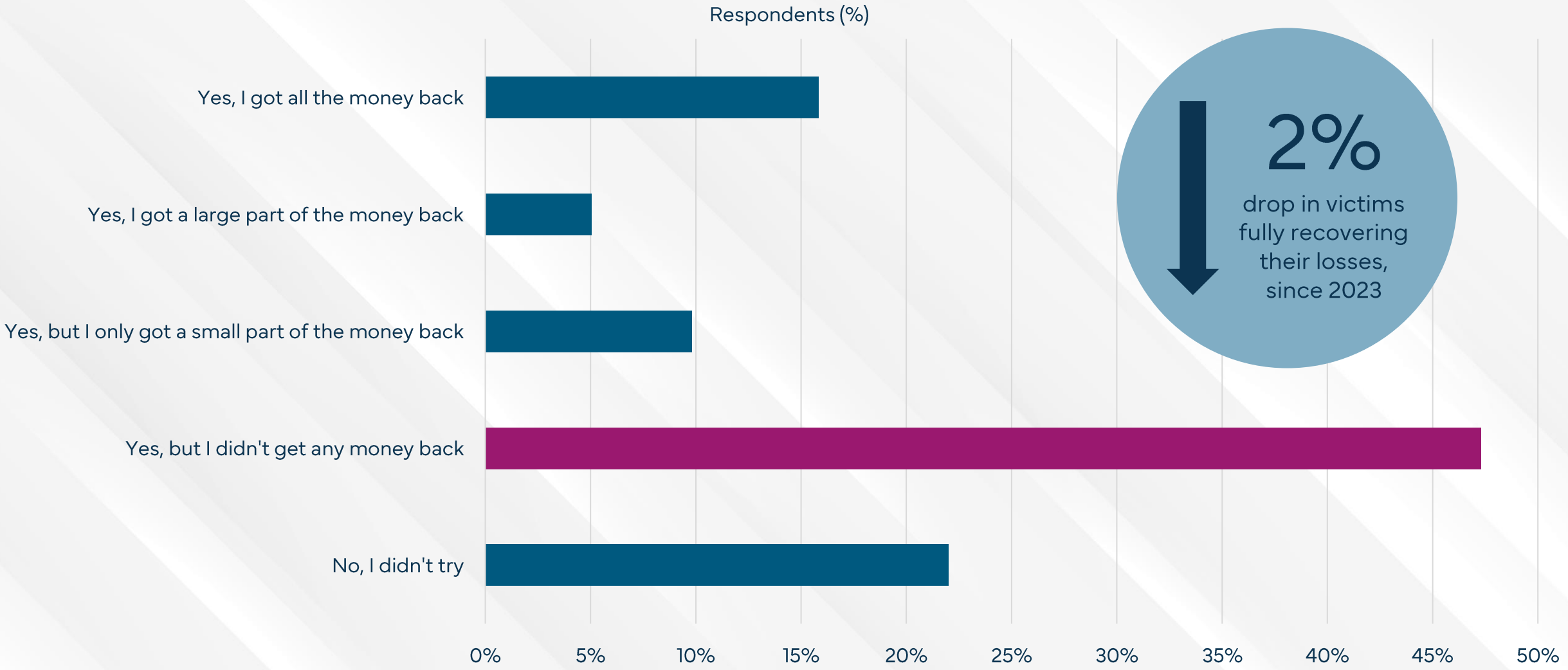
Credit Cards & Bank Transfer are the top scam payment methods



PayPal and peer-to-peer apps are also popular tools which scammers use to collect stolen funds.

Q15 - How did you pay the scammer?

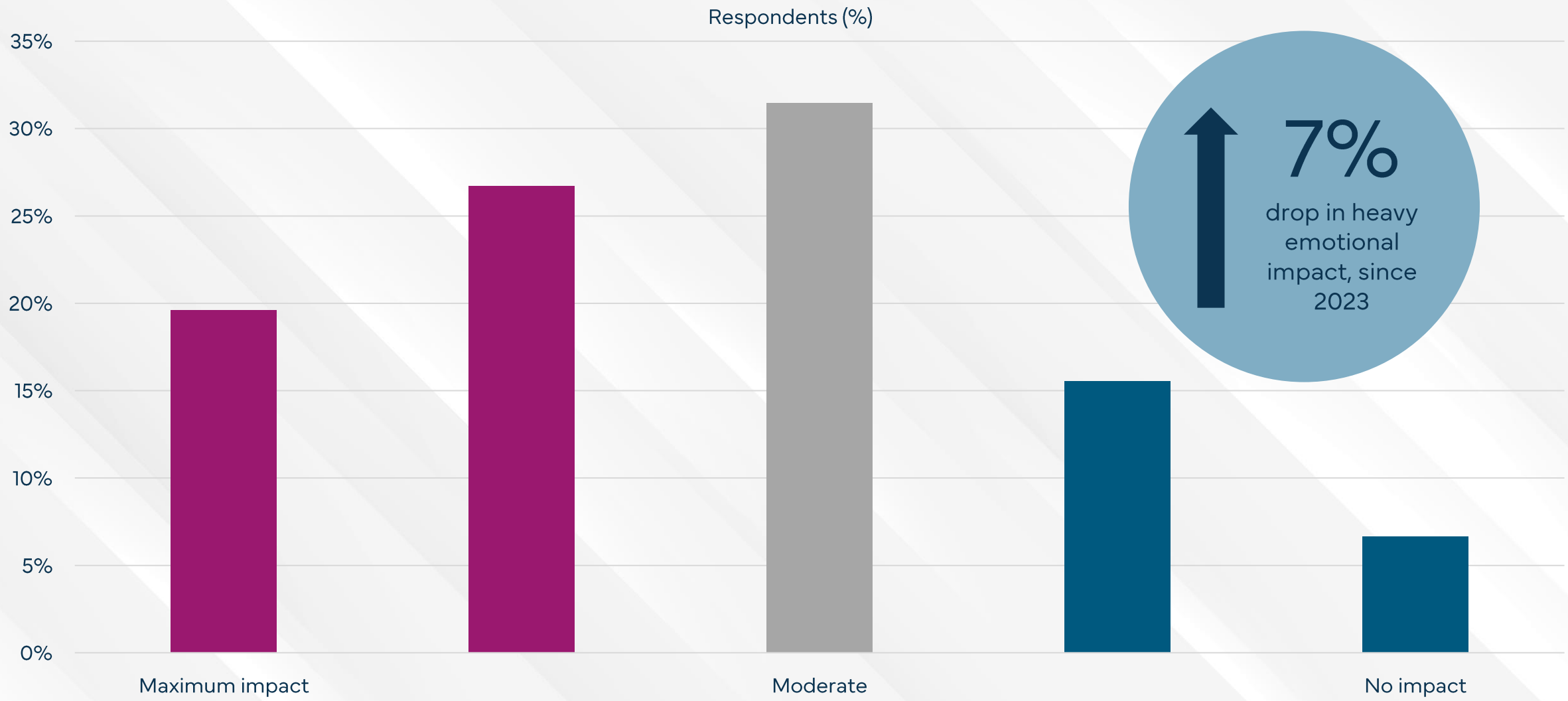
Only 16% of victims were able to fully recover their losses



22% did not try to recover their funds. 47% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

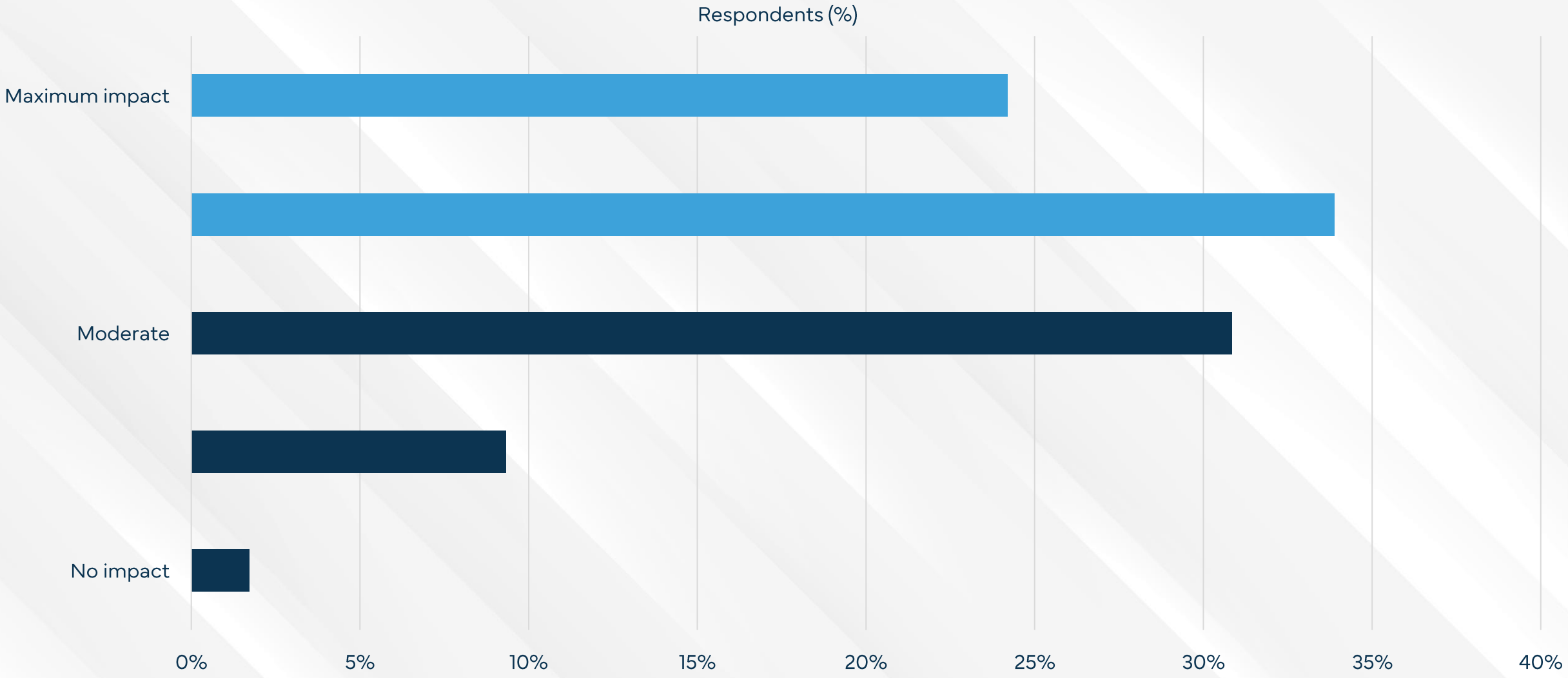
46% of French victims perceived a strong emotional impact



22% of the survey respondents reported little to no emotional impact due to scams.

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

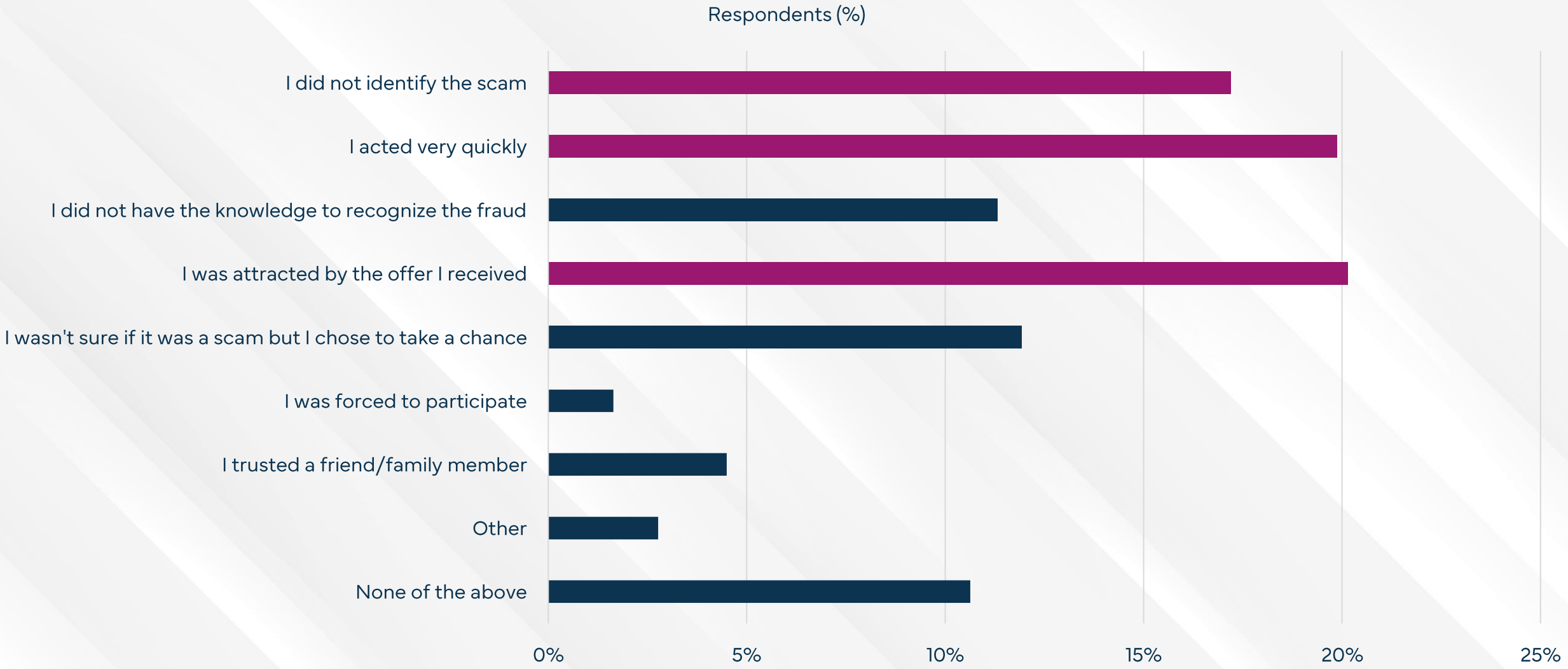
58% of the French have less in trust the Internet because of scams



Only 2% of the French 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?

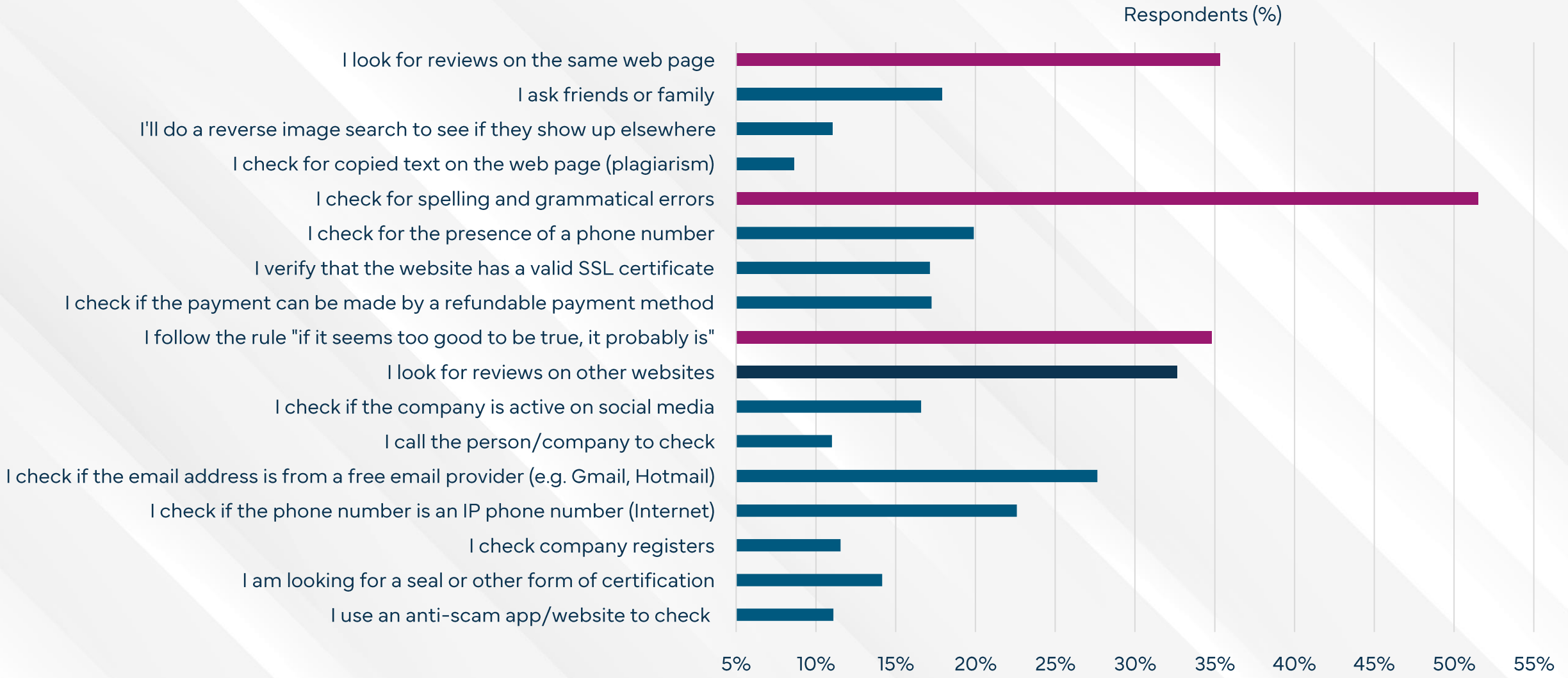
The French get caught out by reacting quickly to attractive offers



A sizable portion of victims also reported that they did not detect the scam until it was too late.

Q19 - What was the main reason you were deceived?

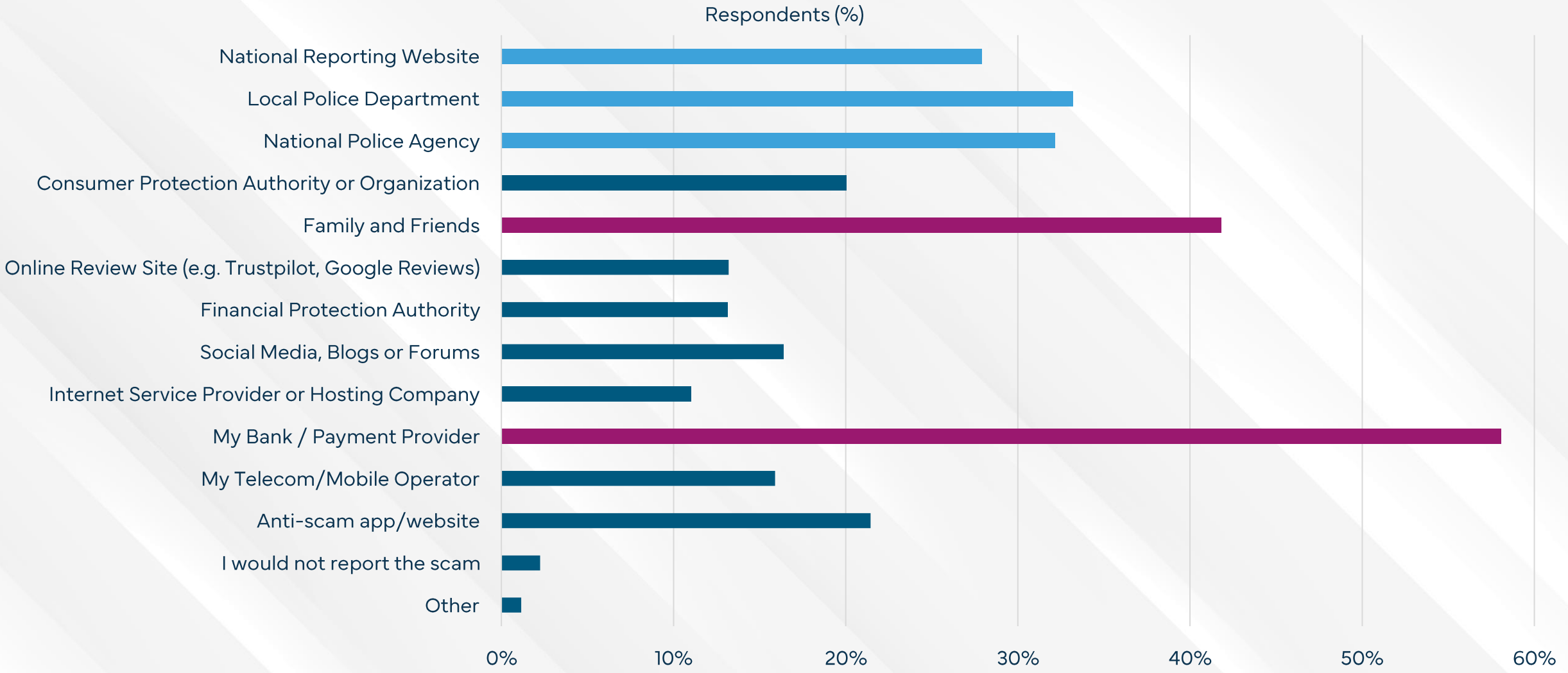
Over half of the respondents rely on spelling & grammatical errors



Many reported checking reviews on the same website and “if it is too good to be true, it probably is” rule.

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

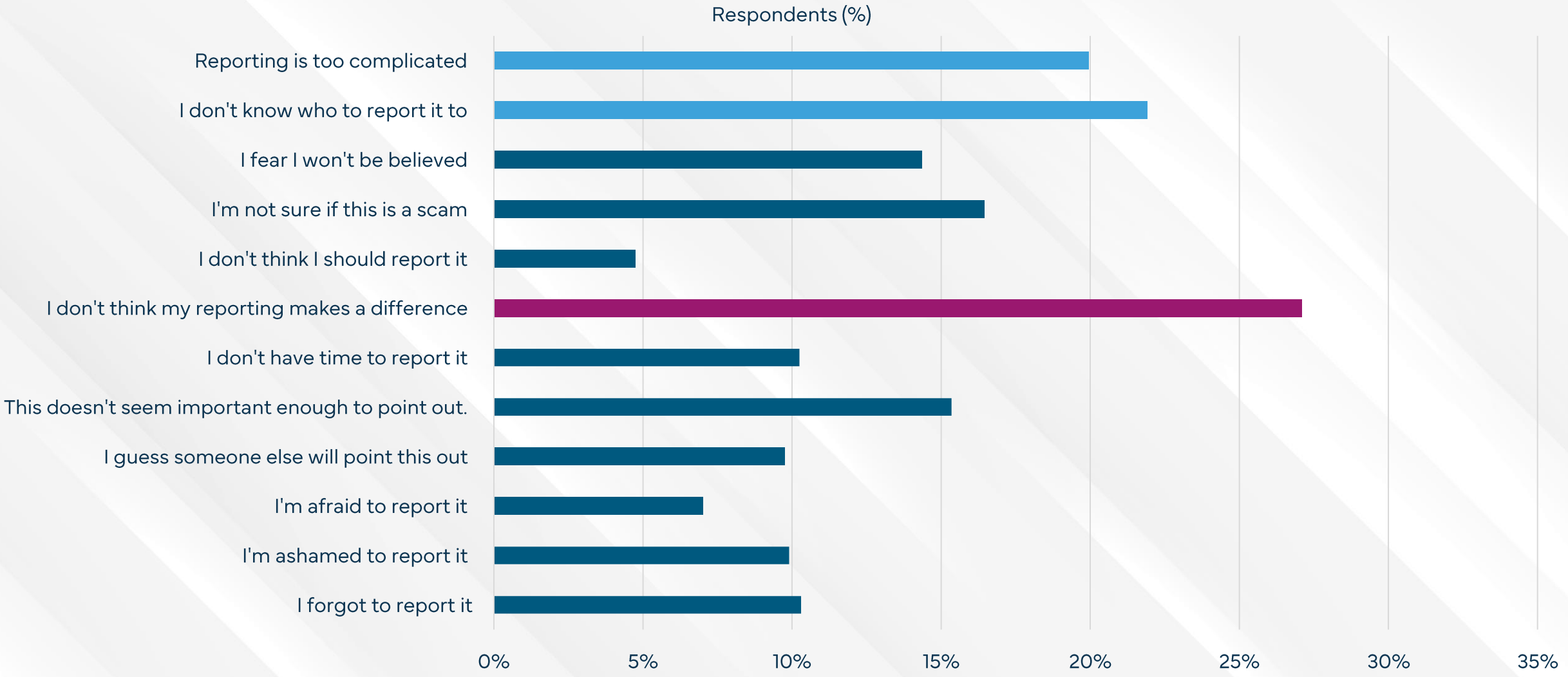
Scams are mostly shared with Banks and Family & friends



Local police stations, national police agency & reporting website are popular places to report scams.

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

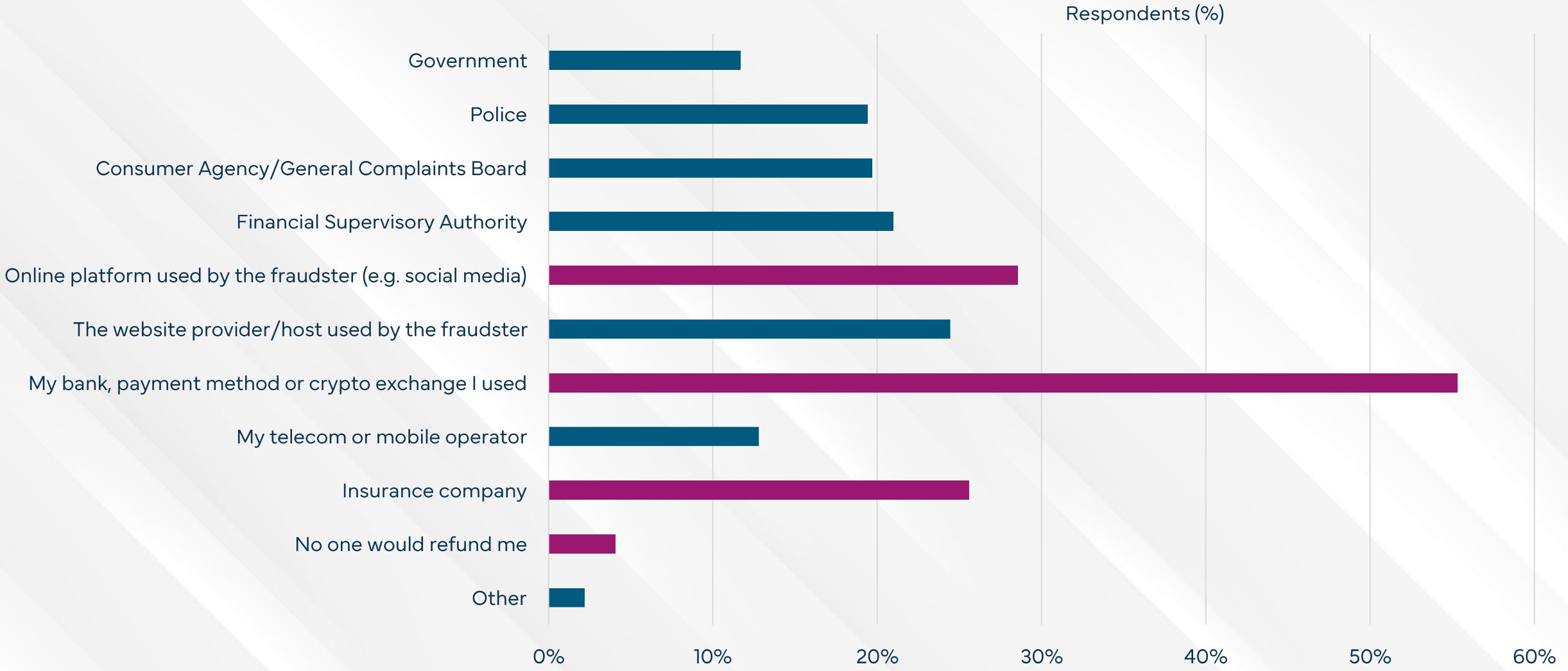
Many French believe that reporting scams won't make a difference



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

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

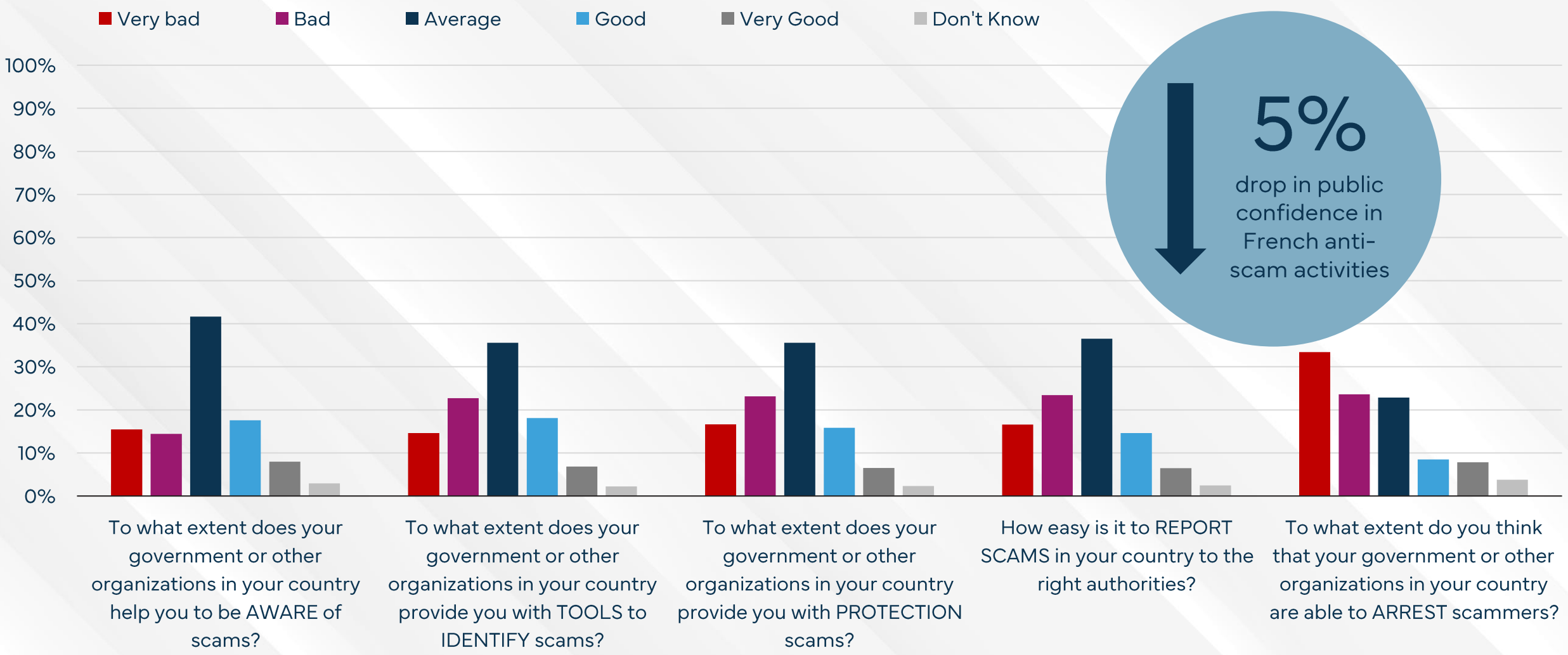
4% of the French assume no one will refund their scam losses



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

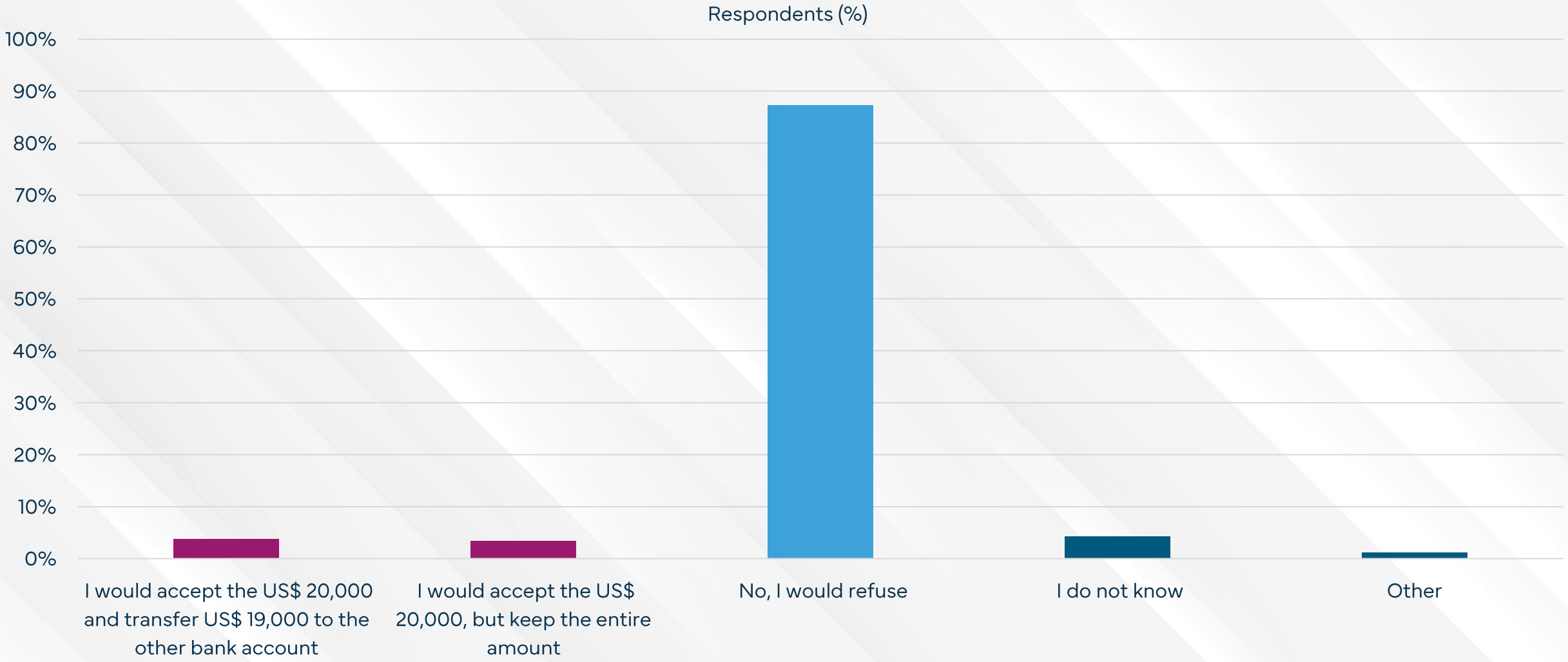
Public opinion is stacked against French efforts to arrest scammers



Overall, 41% of the participants rate French government action as insufficient, while 22% are satisfied.

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 French admit that they would consider being a money mule



However, 87% 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?

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.

BioCatch helps the largest and most recognized financial institutions and telecommunications brands establish trust with their customers, while protecting them from digital fraud. As behavior has become one of the few elements of our digital identities that is truly and uniquely human. By leveraging these behavioral factors, BioCatch provides its clients with powerful and reliable analysis to ensure the authenticity and integrity of transactions.

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.

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