



# The State of Scams in Japan 2024

# Fraudsters target 1-in-3 as Japanese lose USD\$22 billion in 12 months

The 2024 State of Scams in Japan report, produced by the Global Anti-Scam Alliance (GASA) in collaboration with Whoscall and ScamAdviser, offers an in-depth analysis of the scam landscape in Japan. With responses from 921 Japanese citizens, this report highlights critical trends and shifts in scam activity, victim behavior, and public perception over the past year.

A striking 71% of Japanese respondents reported encountering scams at least once per month, an increase of 8% from 2023. This uptick reflects a growing prevalence of scams, indicating that scammers are becoming more aggressive in their outreach. Moreover, 28% of respondents reported experiencing more scam encounters in the last 12 months, suggesting that the environment for fraud is becoming increasingly hostile. This increase, coupled with only 22% of respondents experiencing a reduction in scam encounters, points to a need for more effective countermeasures.

Despite a modest increase in scam recognition confidence—up 5% from 2023 to 27%—the majority of Japanese remain wary of their ability to detect scams, with 37% expressing a lack of confidence. This disparity highlights a significant vulnerability: a large portion of the population feels ill-equipped to identify scams, making them prime targets for fraudsters. The high levels of uncertainty about scam tactics, especially involving AI technologies, further exacerbate this issue, as 43% of respondents were unsure if AI was used to scam them.

Scammers in Japan continue to exploit digital communication channels, with a 10% rise in text/SMS message scams since 2023. Texts, emails, and social media platforms such as Gmail, Amazon, and Facebook remain the most exploited, demonstrating that

scammers are leveraging widespread and trusted digital tools to reach potential victims. The rise in scams on platforms like Facebook shows no sign of slowing.

The financial toll of scams in Japan is severe, with 39% of participants losing money to scams. The average loss per victim stands at \$2,334, contributing to a staggering total national loss of \$22 billion USD (3.22 trillion JPY). This equates to 0.5% of Japan's GDP, a significant economic burden that reflects not only the financial costs but also the broader societal impact of scams. The data suggests that Japan's economic landscape is heavily affected by scams, warranting urgent attention from both the private sector and government entities.

Only 5% of scam victims were able to recover their losses, a decline of 2% from the previous year. This low recovery rate indicates a gap in effective support mechanisms for victims, who largely feel disempowered to reclaim their stolen funds. Furthermore, 87% of Japanese did not report scams to law enforcement, a 5% increase from 2023. This underreporting is likely driven by a combination of factors: a lack of trust in authorities, perceived inefficacy of reporting, and uncertainty about the reporting process. The fact that many Japanese do not believe that reporting will make a difference suggests a systemic issue in the response infrastructure.

The emotional toll of scams is becoming more pronounced, with 45% of victims experiencing a strong emotional impact—an increase of 7% from 2023. This rise in psychological distress is likely due to both the financial losses and the violation of trust that scams represent. Additionally, 61% of Japanese reported a loss of trust in the Internet because of scams, signalling a broader impact on public confidence in digital

interactions. This poses a long-term risk to Japan's digital economy and its integration of new technologies.

The data underscores a critical need for more robust public education and stronger government interventions. The dissatisfaction with the government's efforts—66% of respondents rated these efforts as poor—reflects a public demand for more decisive action. In a test of honesty, only 1% of Japanese admitted that they would consider becoming money mules, which is one of the lowest rates in the world.

As scams become more prevalent and sophisticated, Japan faces significant challenges in both preventing scams and supporting victims. There is an urgent need for coordinated efforts to enhance scam awareness, improve reporting and recovery processes, and restore public trust in digital platforms and governmental responses. Addressing these challenges will require a multifaceted approach, combining technology, education, and policy reform to protect Japanese citizens from the evolving threats of fraud.



Jorij Abraham  
Managing Director



Sam Rogers  
Director of Marketing

ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). ScamAdviser provides real-time detection of suspicious activity and scam prevention for websites, calls, messages, and online platforms. With the world's largest scam database, ScamAdviser partners with over 400 organizations to protect more than 1 billion consumers worldwide, helping people confidently navigate the digital world. In this interview, Aaron Chiou, Product Director of ScamAdviser, will describe the current state of scams in Japan and the advanced strategies needed for enterprises to protect consumers.

How significant has the issue of scams become in Japan?

Scams have become an increasingly serious issue in Japan, with 71% of citizens encountering scams at least once a month, marking an 8% increase compared to the previous year. Despite this high exposure, only 27% of the population feels confident in identifying scams, leaving a significant portion of the public vulnerable. Although most Japanese are aware scammers can use AI against them, the growing use of AI-generated content has further complicated the ability to recognize deceptive

schemes, underscoring the urgent need for improved public education and more advanced detection tools to safeguard citizens.

What types of scams have trended in Japan recently?

In Japan, scam trends involve various tactics primarily delivered through digital channels such as text messages, emails, phone calls, and social media. Notably, Gmail has surpassed Amazon as the most frequently targeted platform, reflecting a change in how scammers engage with potential victims. Social media platforms like Instagram, X (formerly Twitter), and Facebook are also among the top five platforms where users encounter scams. Identity theft is the most common scam in Japan, with bank and wire transfers being the primary payment methods used by scammers. Personal information is stolen for financial fraud or impersonation, making it crucial to protect banking and personal data.

Which actions have been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn?

The Japanese government has set up anti-scam measures, promotes international cooperation, and encourages transactions with certified companies. However, despite these efforts, an overwhelming 87% of scam victims do not report incidents to authorities, reasons include doubts about identifying scams and the uncertainty of where to report them. Only 5% manage to

fully recover their losses. To address this, telecom operators and retailers, in collaboration with the TrustTech company, try to prevent scams by launching caller ID apps that help consumers identify malicious calls.

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

To effectively combat scams, sectors such as government, banks, and telecoms should educate consumers and provide them with self-protection tools. Additionally, integrating anti-scam solutions into existing platforms can help verify trustworthy contacts and prevent scams. AI-based scam detection can identify suspicious activities, and simplifying reporting and recovery options would encourage more victims to seek help. Strengthen protection requires governments to collaborate across industries and stakeholders to create a safer digital space.



Aaron Chiou  
Product Director



Whoscall, powered by Gogolook, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, and links.

In the Japan 2024 State of Scams report, GASA interviewed Weichen Lo, Japan Country Head of Whoscall, to share insights on the in-depth analysis of the evolving scam landscape in Japan, to equip consumers with the knowledge and tools they need to stay one step ahead of scammers.

## How significant has the issue of scams become in Japan?

In Japan, the issue of phishing and scams has reached critical levels. In 2023, the total annual damage from various scams exceeded 211 billion yen. Among these, specialized scams phone calls accounted for more than 45.2 billion yen, while romance scams and social media-based investment fraud led to losses of over 45.5 billion yen. Phishing-related damages also surged tenfold, reaching over 8.7 billion yen. Additionally, the unauthorized outflow of one cryptocurrency market company due to suspected phishing attacks resulted in losses of approximately 48 billion yen. This trend reflects the increasing sophistication of scam schemes in Japan.

## What types of scams have been trending in Japan recently?

In Japan, investment scams and fake ad scams on social media have surged, and the issues of brand infringement and celebrity impersonation have attracted significant attention. These scams exploit users through fraudulent advertisements, causing significant financial losses of over 45.5 billion yen in 2023. In addition, scam phone calls and phishing attacks are also on the rise, affecting a wide range of consumers. In addition, phishing scams impersonating government agencies such as the National Tax Agency and My Number Portal have increased rapidly this year. In these scams, victims are directed to fake websites by phishing emails or SMS messages, and their login and credit card information are stolen in a growing number of cases.

## Which actions have been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn?

The Japanese government has taken several actions to protect consumers from scams, including launching public awareness campaigns, strengthening regulations, and improving cybersecurity measures. A best practice is the proactive educational efforts made by government agencies to raise scam awareness among consumers. Additionally, collaborations between law enforcement, private companies, and tech providers have also been crucial. For example, we partner with many local city governments and telecommunications companies to expand Whoscall services and scam prevention

awareness, demonstrating the power of public-private cooperation in combating scams.

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

To empower consumers in the fight against scams, it is crucial to raise public awareness about new scam tactics and provide access to tools like Whoscall. Whoscall helps users protect themselves from spam calls, phishing websites, and other fraudulent activities by verifying phone numbers and identifying suspicious communications.

We encourage consumers to verify phone numbers and suspicious messages using the Whoscall app and assess website risks with tools like SAGICHECK. Finally, consumers should feel comfortable consulting family members, local authorities, or law enforcement if they suspect fraudulent activity. Strengthening collaboration between the public and private sectors is key to building trust and effectively combating scams.

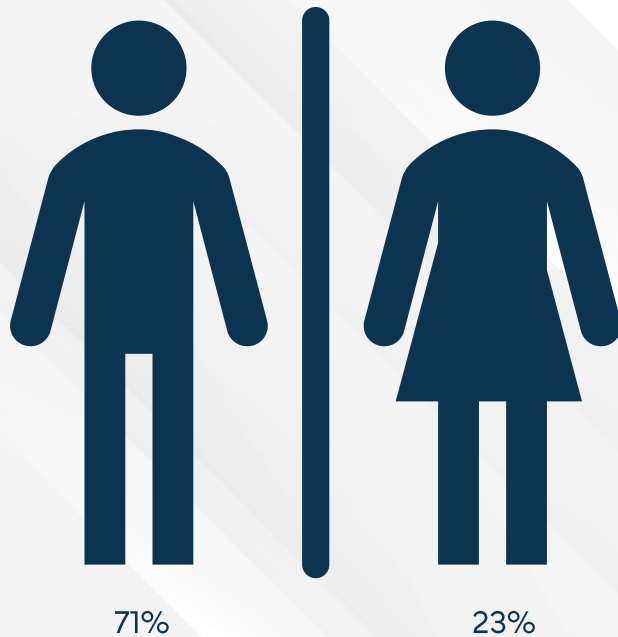


Weichen Lo  
Japan Country Head  
of Whoscall

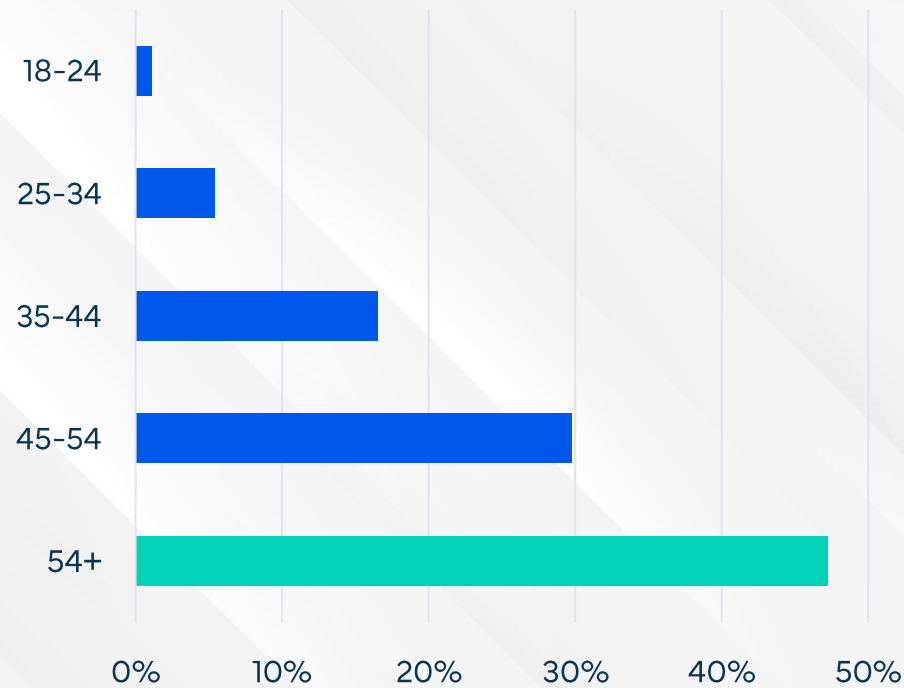
**whoscall**

# 921 Japanese citizens completed the State of Scams survey

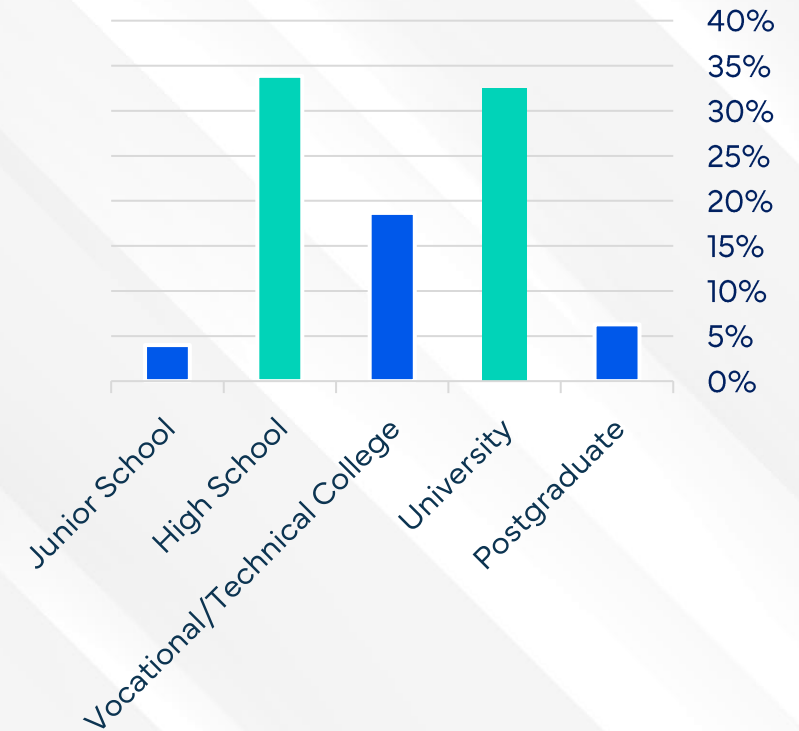
### Gender



### Age Range

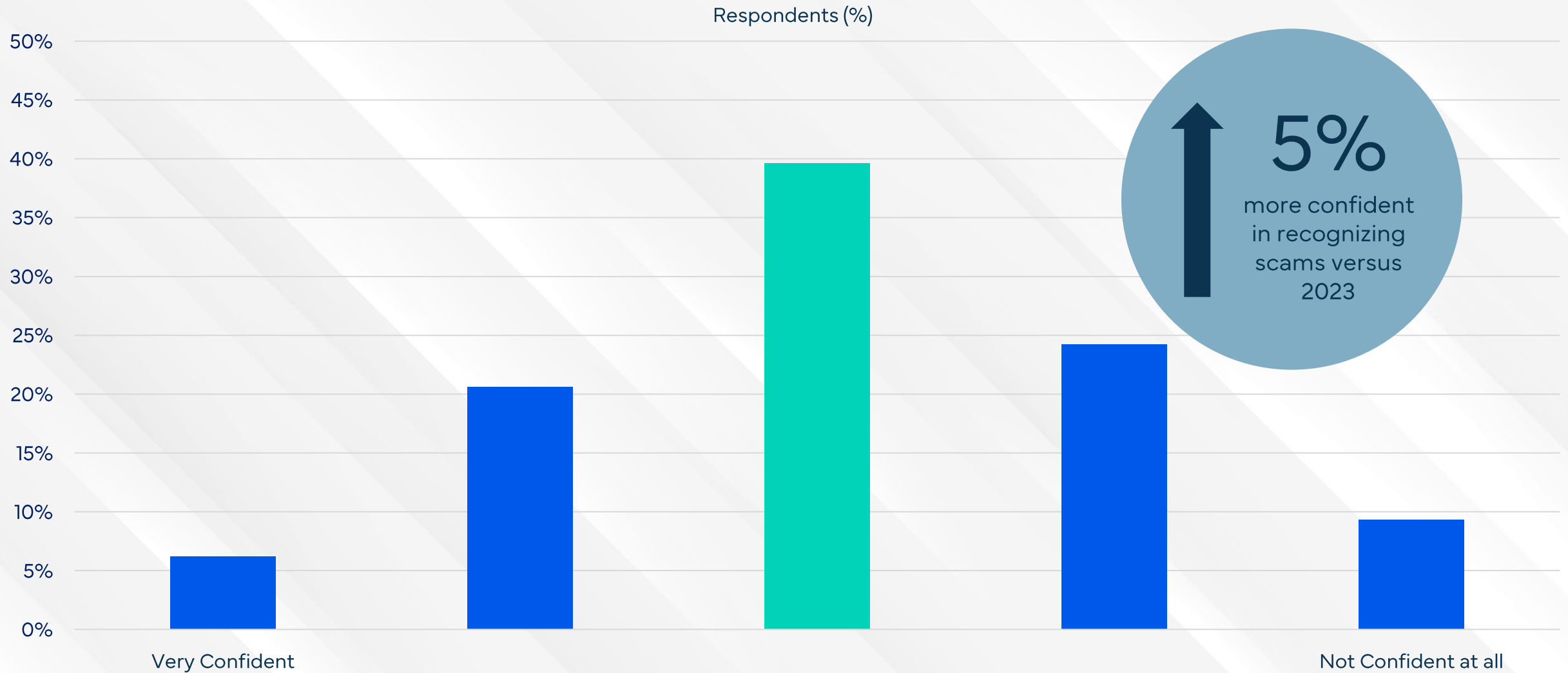


### Education



The State of Scams in Japan 2024 survey was responded to by significantly more men than women. The majority of which were over 45 years old with a high school or university education.

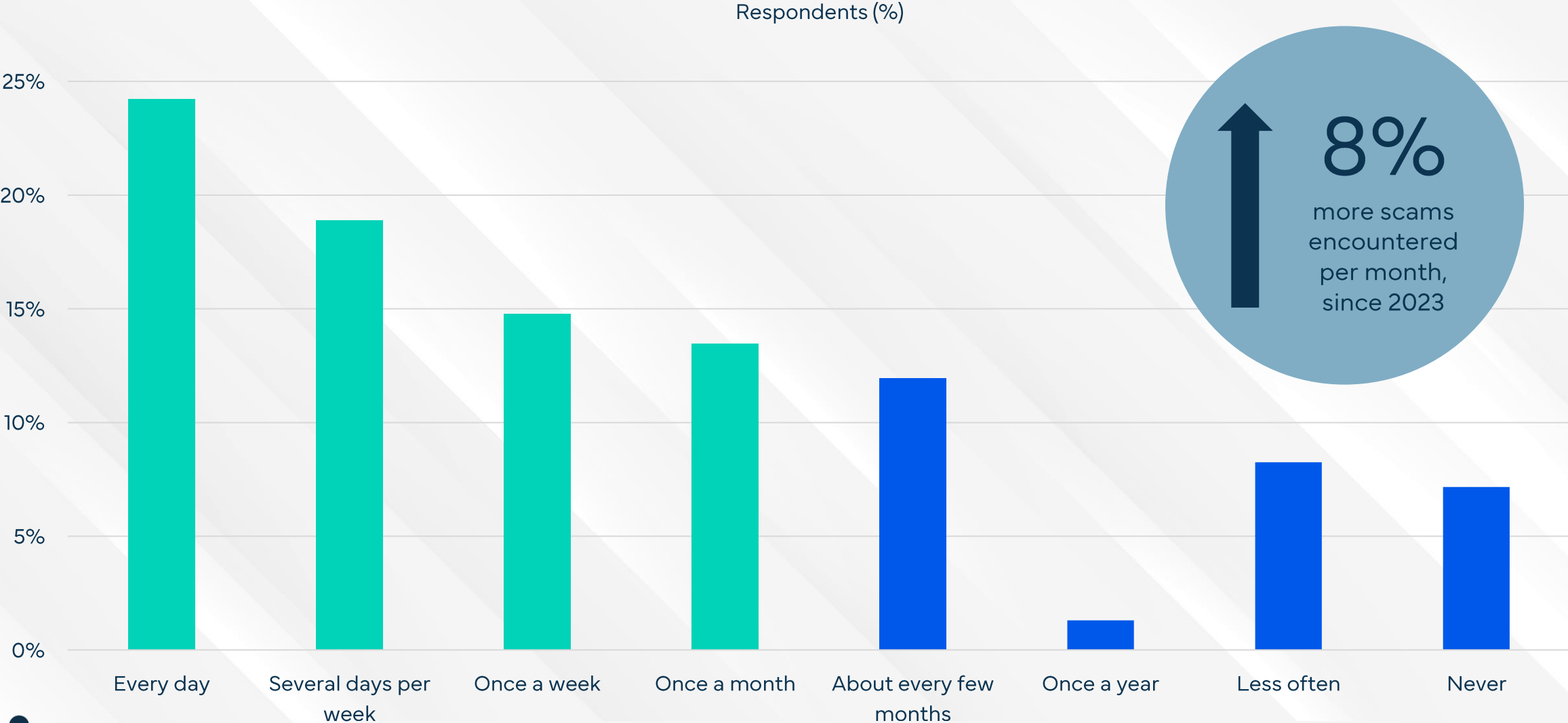
# 27% of Japanese are confident in their ability to recognize scams



37% of the respondents reported feeling a lack of confidence in recognizing scams.

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

# 71% of Japanese encounter scams at least once per month



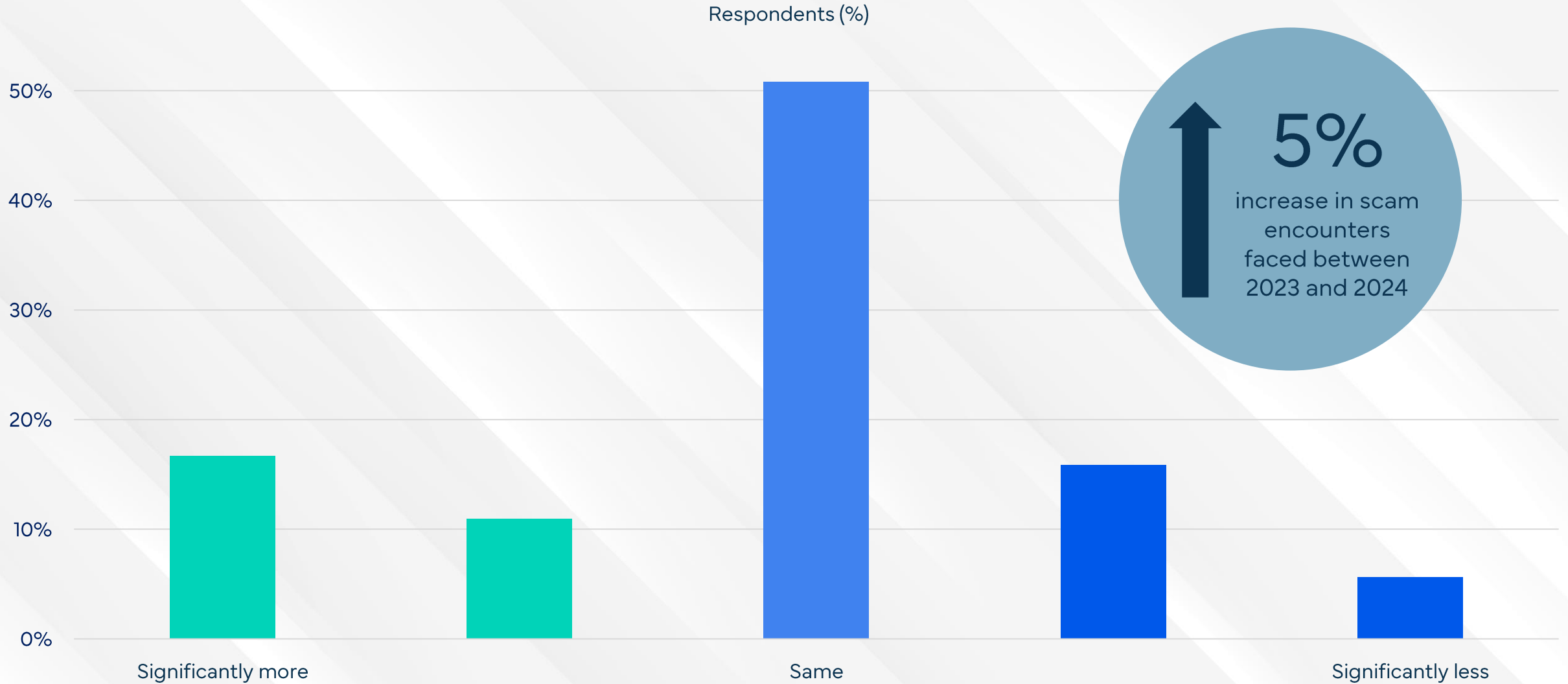
↑  
**8%**  
more scams  
encountered  
per month,  
since 2023



15% of Japanese 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.

# 28% of Japanese faced more scam encounters in the last 12 months

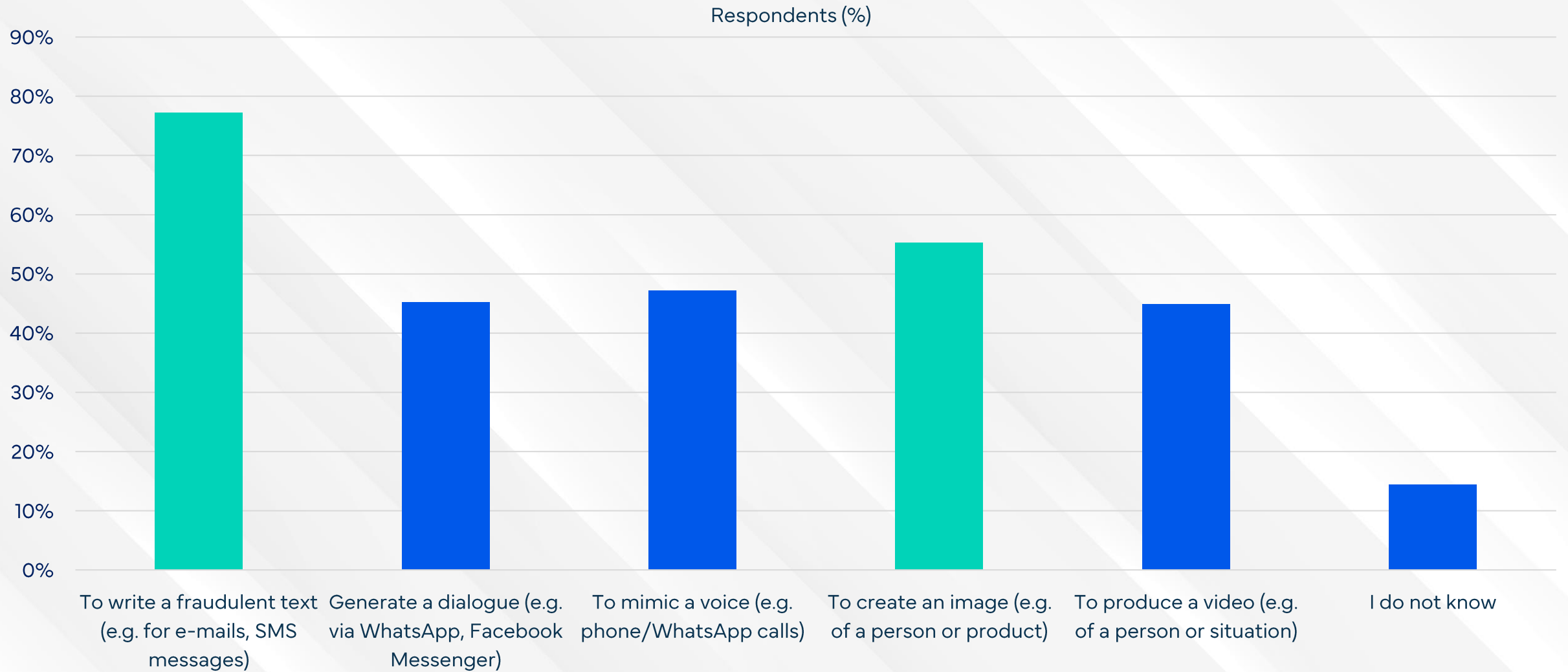


Only 22% of Japanese respondents experienced a reduction in scam encounters in the past 12 months.

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?



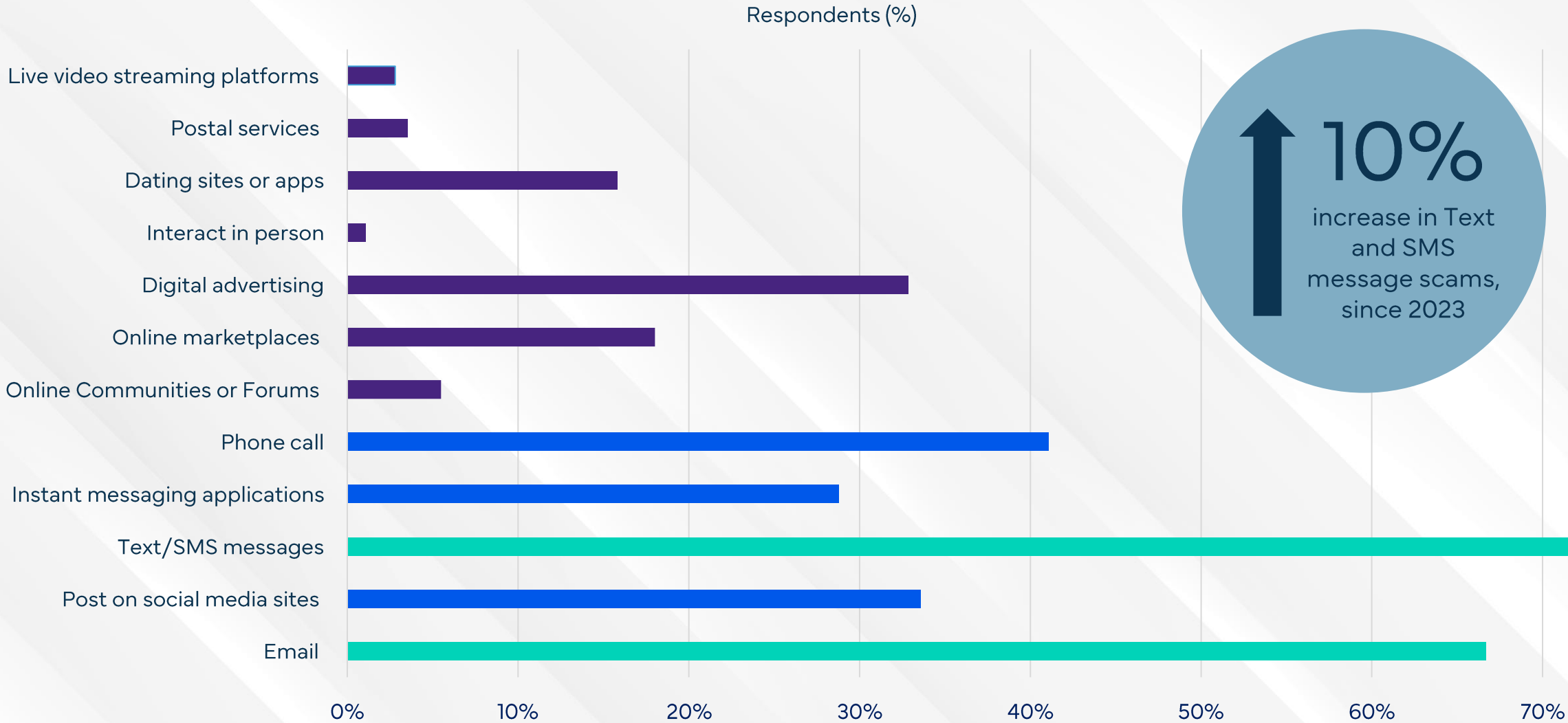
# Most Japanese are aware scammers can use AI against them



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

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

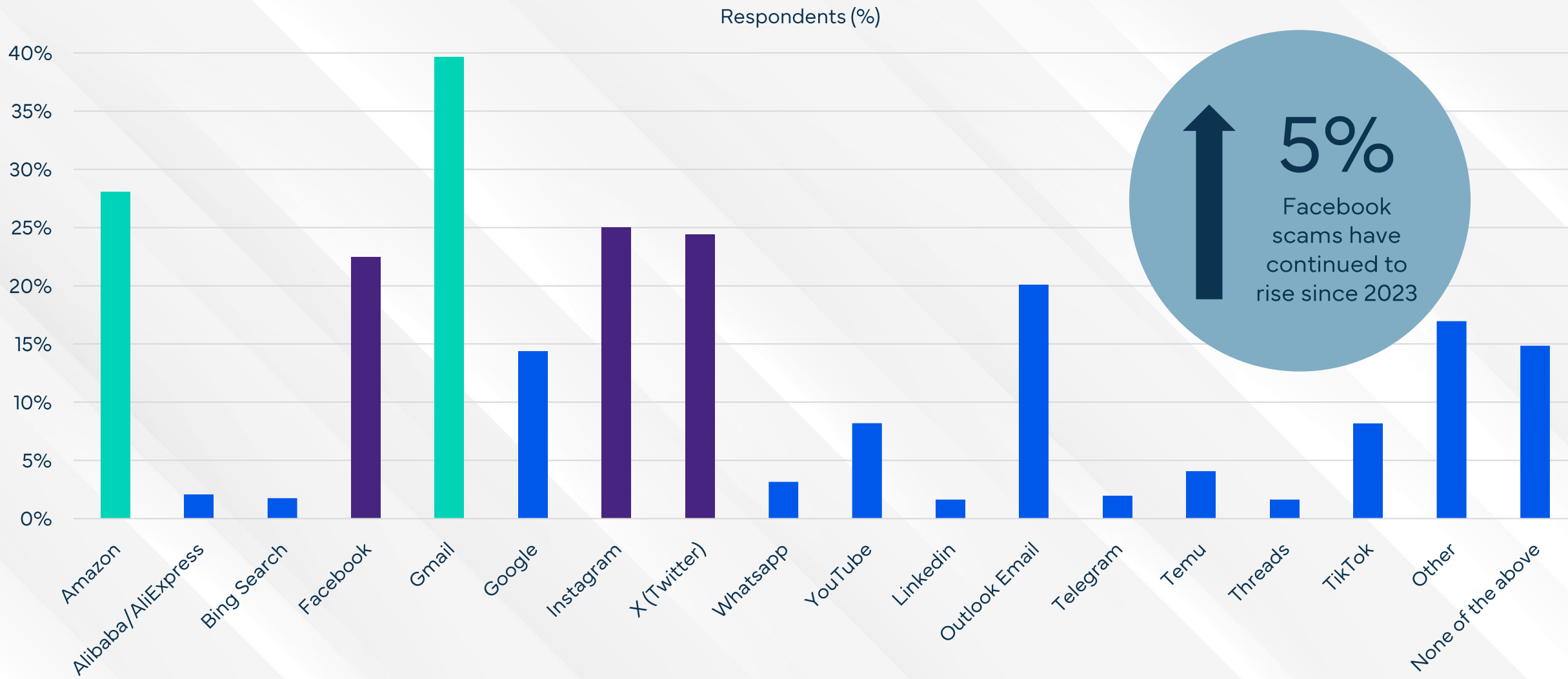
# Majority of scams are delivered via text/SMS message & email



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

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

# Gmail overtakes Amazon as the platform most exploited by scammers



↑  
**5%**  
Facebook  
scams have  
continued to  
rise since 2023



Instagram, X (Twitter), and Facebook round out the top five platforms where people encounter scams.

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

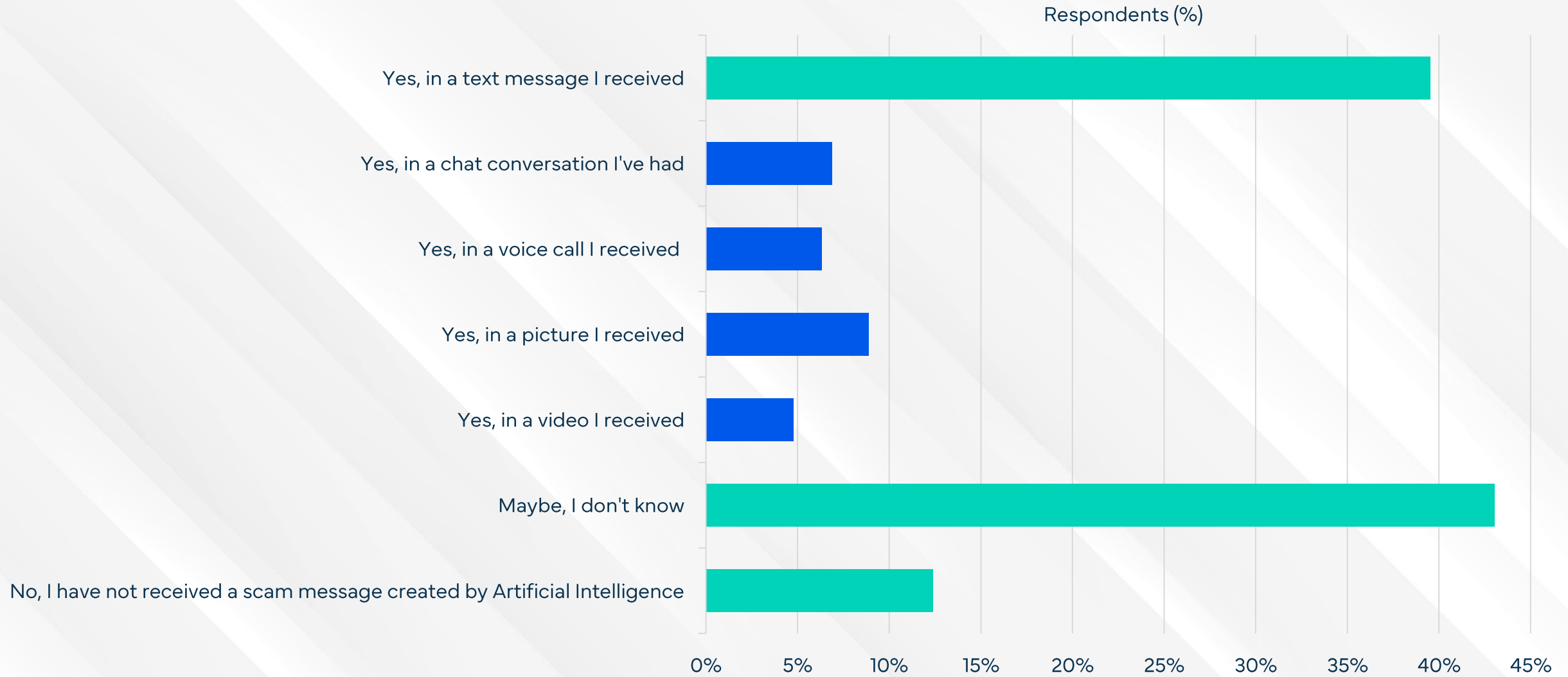
# 87% of Japanese did not report the scam to law enforcement



10% stated that they 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?

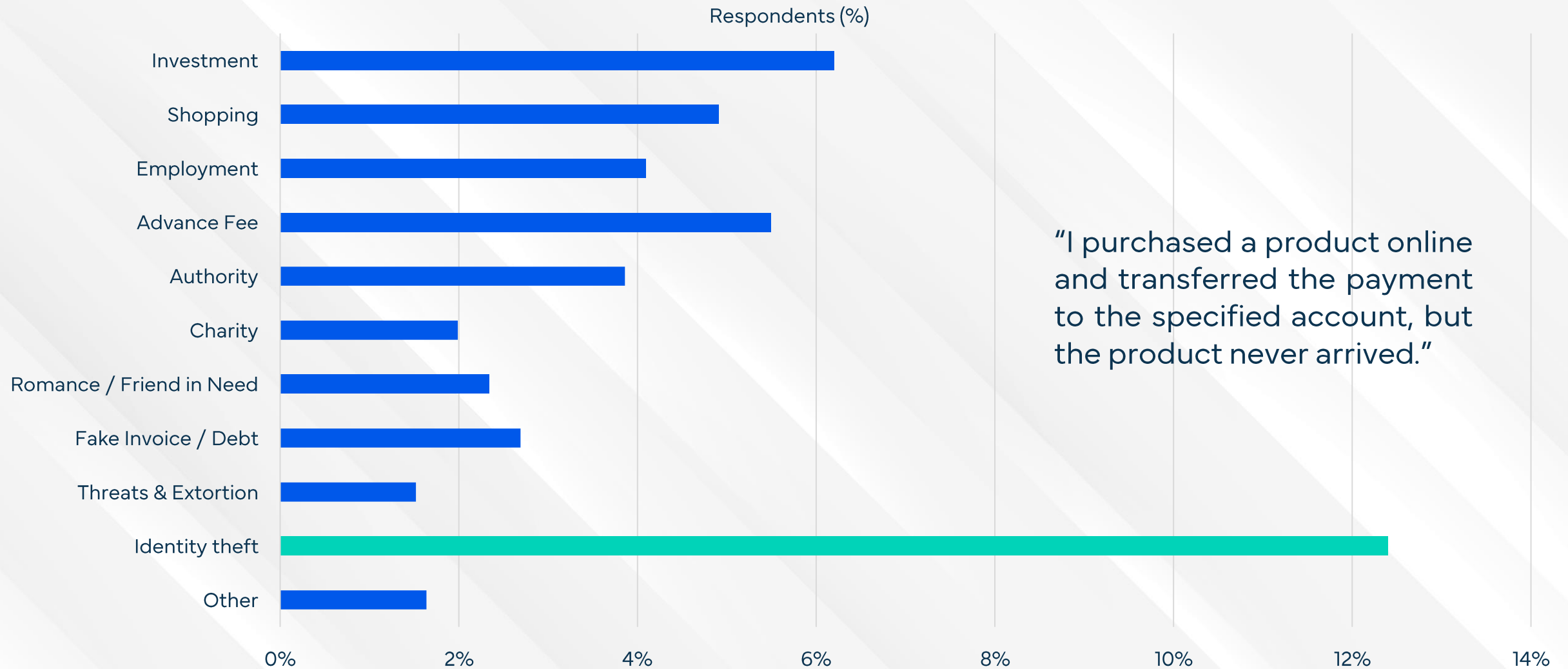
# 43% of Japanese were uncertain whether AI was used to scam them



12% of Japanese 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?

# Identity Theft is the most common type of scam in Japan



74% did not fall victim to the most common scams in the last year. 0.47 scams were reported per victim.

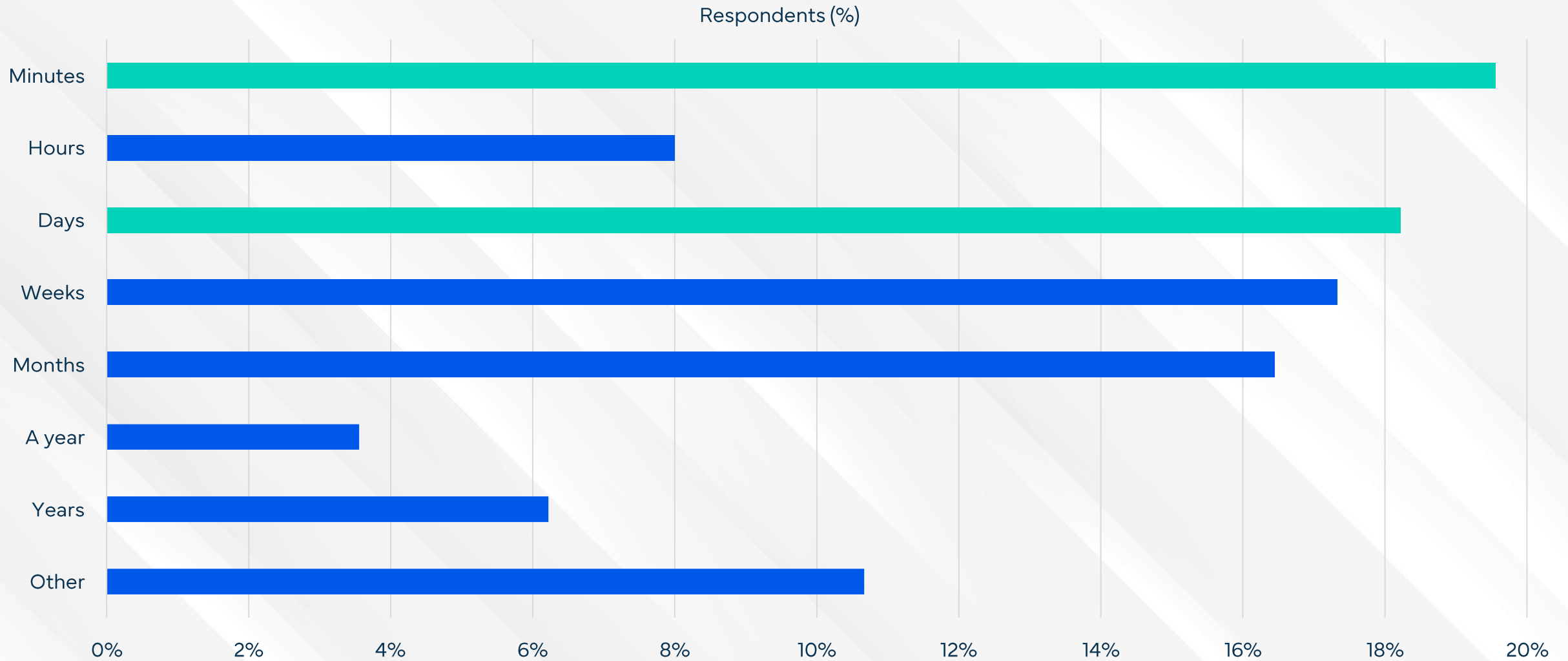
Q10 - Which of the following negative experiences happened to you in the last 12 months?

"I was told I had won a huge amount of money and was pressured to complete the procedure, and although they said it was free, (afterwards) they insisted I pay with a gift card and said I would be arrested if I didn't pay."

"I was approached via Facebook Messenger by a woman who lived in Taiwan and claimed to be the CEO of the Hyatt Taipei, who approached me about investing. I fell for her sweet talk, and ended up being scammed out of 1.34 million yen."

"They called me on a Saturday evening, saying that they were a special investigative agency commissioned by the government, and that ransomware had been used to infect an unspecified number of mobile phones via my email. They let me listen to the audio of them working, and told me that they were cooperating with the investigation to guarantee my safety. I was scammed out of 300,000 yen in a claim for just-in-case insurance."

# 28% of scams are completed within 24 hours of first contact

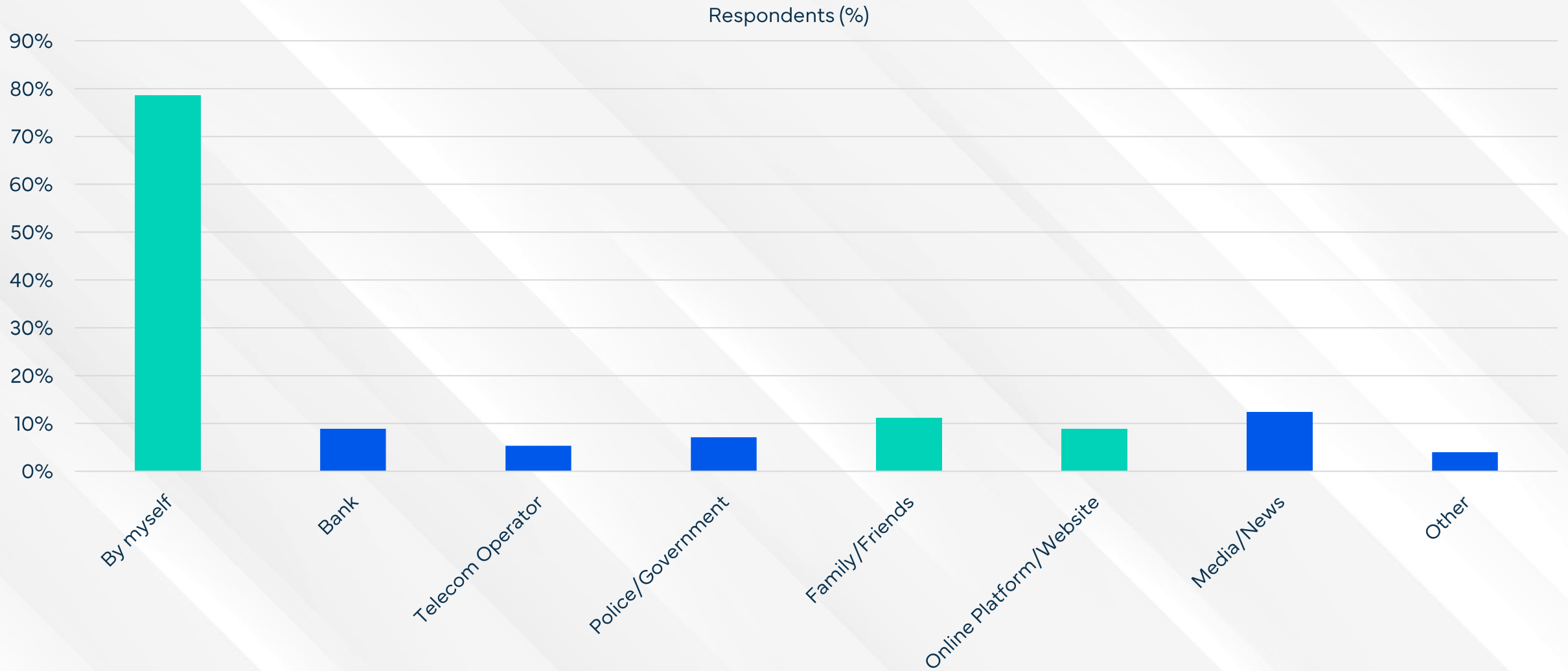


20% reported scams that were over in minutes, while 10% were scammed over a year or more.

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?



# 79% came to their own conclusion that they had been scammed

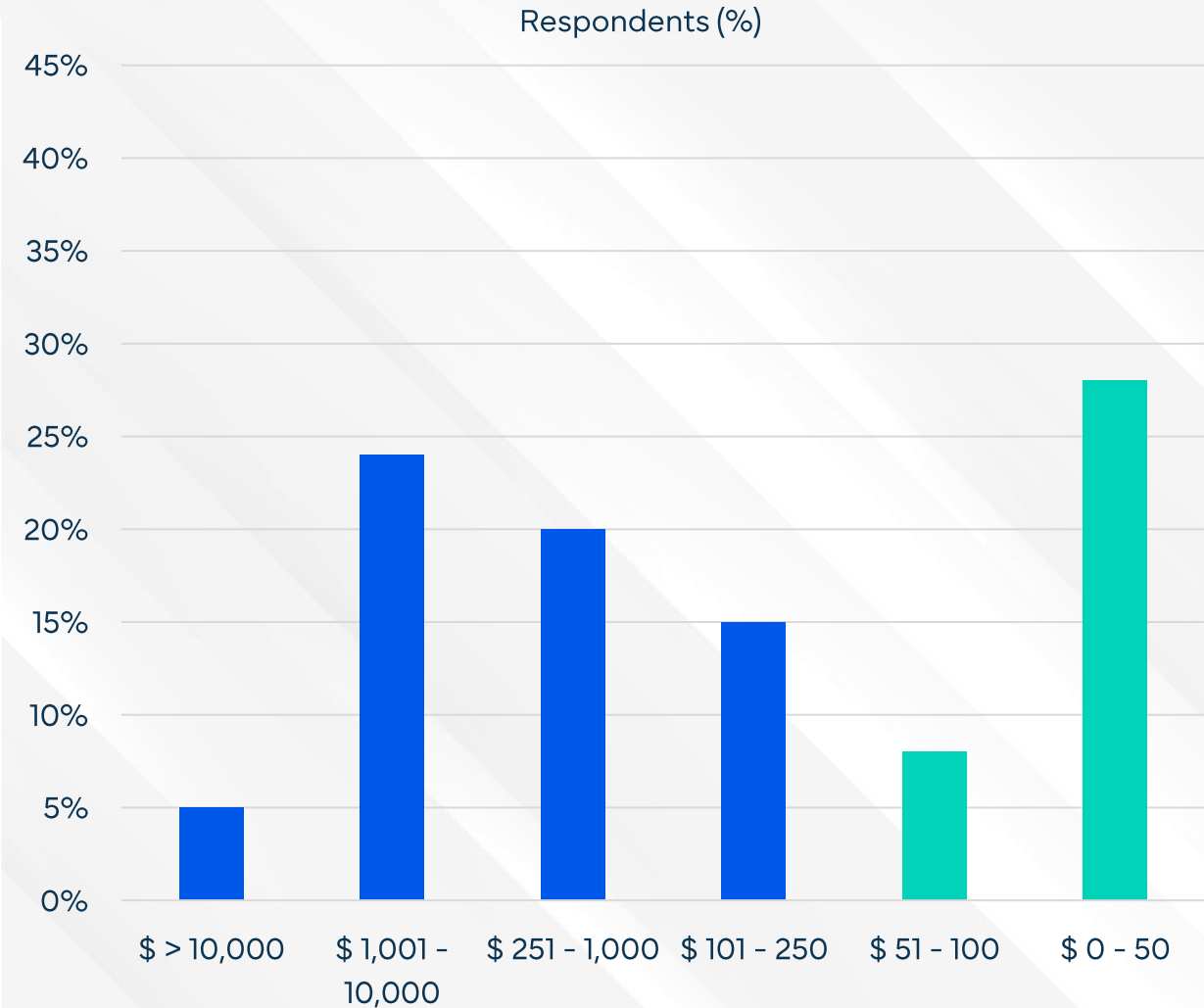


Others were informed by media/news while family/friends are also key in pointing out scams.

Q13 How did you discover you were scammed?

# In total, 39% of Japanese participants lost money to a scam

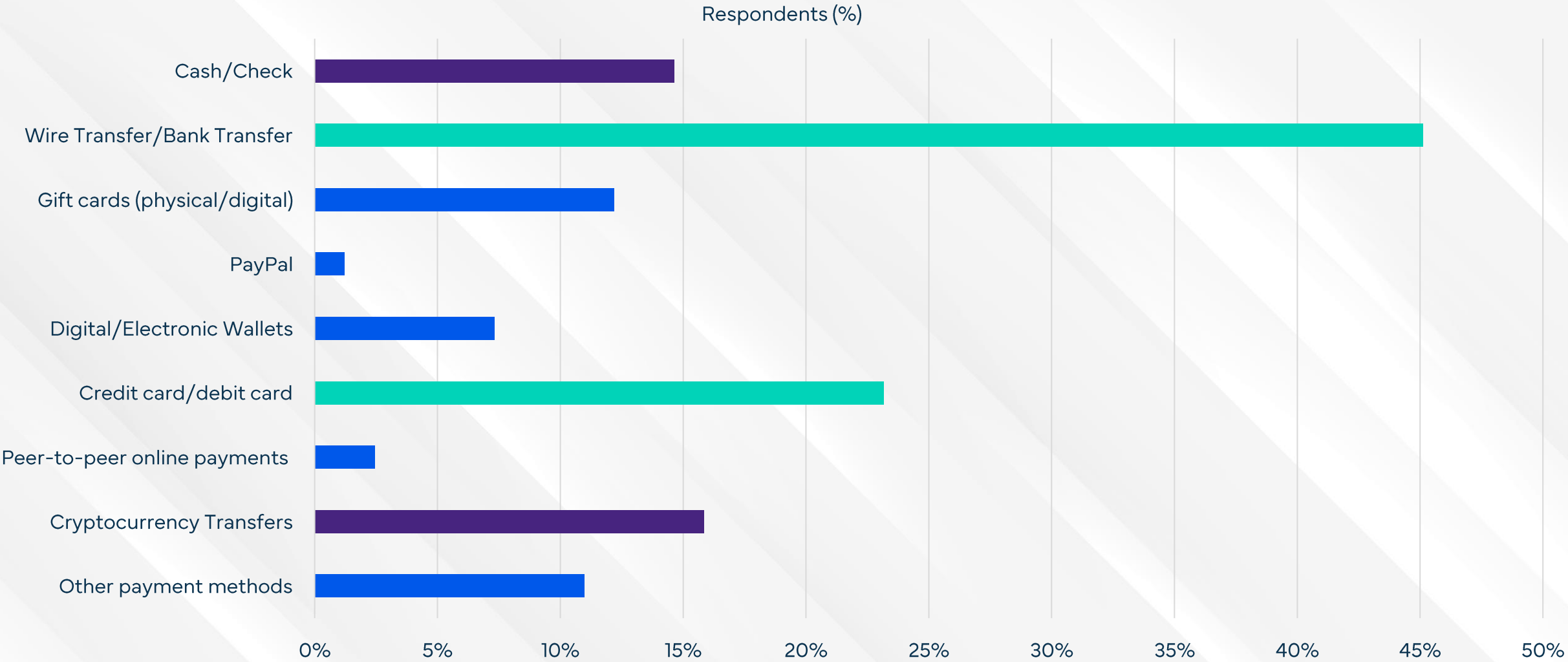
Survey Key Statistics	
Persons approached	921
Participants losing money	82
% losing money / approached persons	9%
Average amount lost in US Dollars	2,334
Total country population	123,201,945
Population over 18 years	104,842,118
# of people scammed > 18 years	9,334,477
Total scam losses (USD)	21,986,670,228
Total scam losses (JPY YEN)	3,216,767,116,470
Gross Domestic Product (USD, millions)	4,230,862
% of GDP lost in scams	0.5%



In total, the Japanese lost \$22 billion to scams, which is equal to 0.5% of Japan's GDP.

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

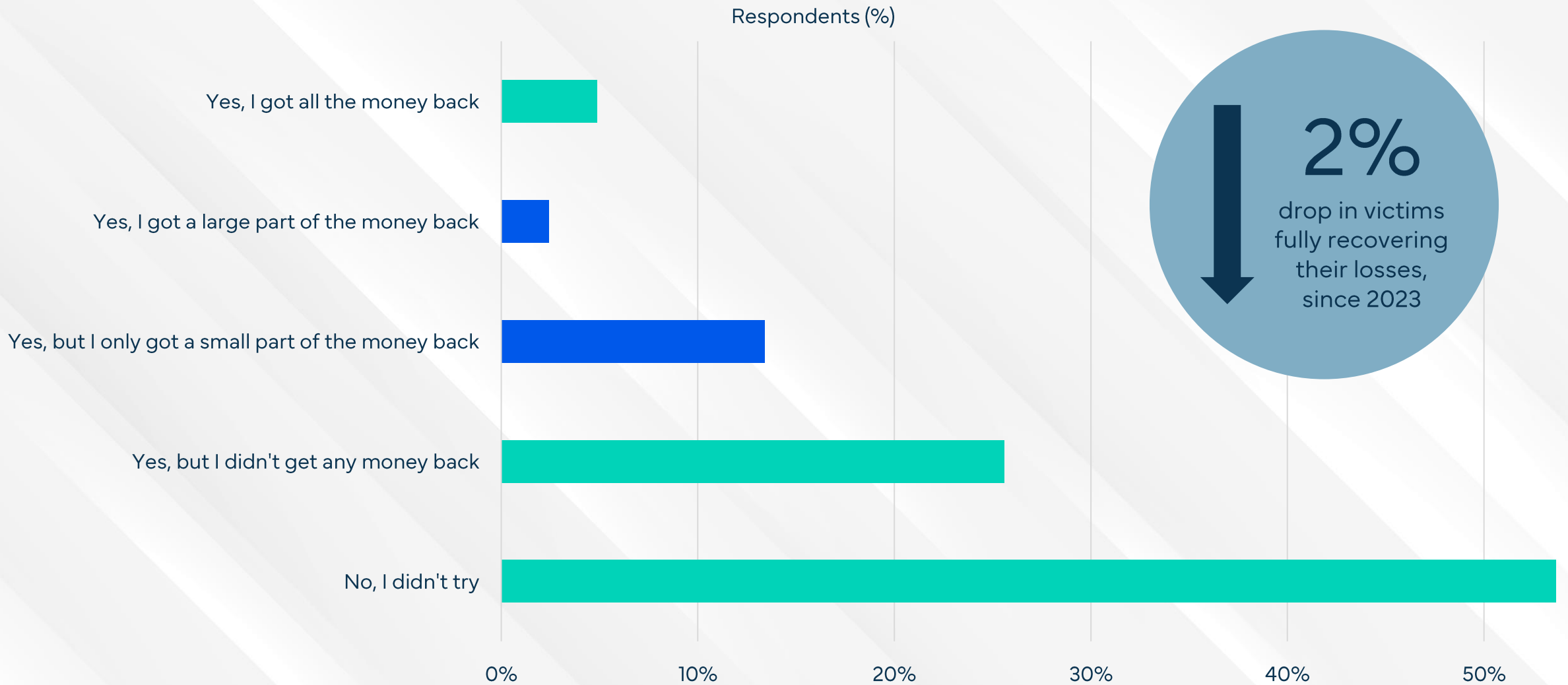
# Bank/wire transfers are the leading scam payment method



Credit/debit cards, cryptocurrencies & cash/checks are also popular methods of payment in fraud cases.

Q15 - How did you pay the scammer?

# Only 5% of victims were able to fully recover their losses



54% did not try to recover their funds. 26% made an attempt, but were not able to recover any money.

Q16 - Did you try to recover the money lost?

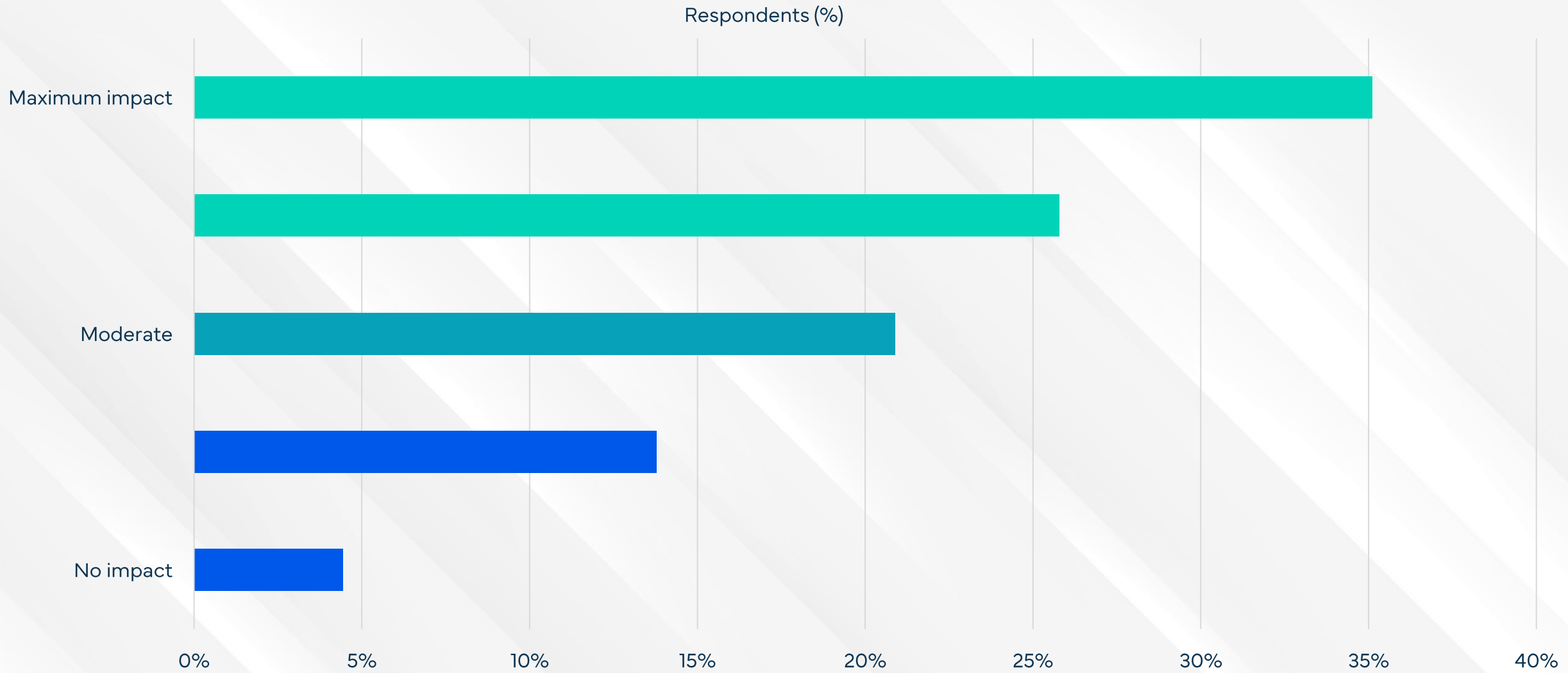
# 45% of the scam victims perceived a strong emotional impact



28% of the survey respondents reported little to no emotional impact due to scam experiences.

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

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



Only 18% of Japanese 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?

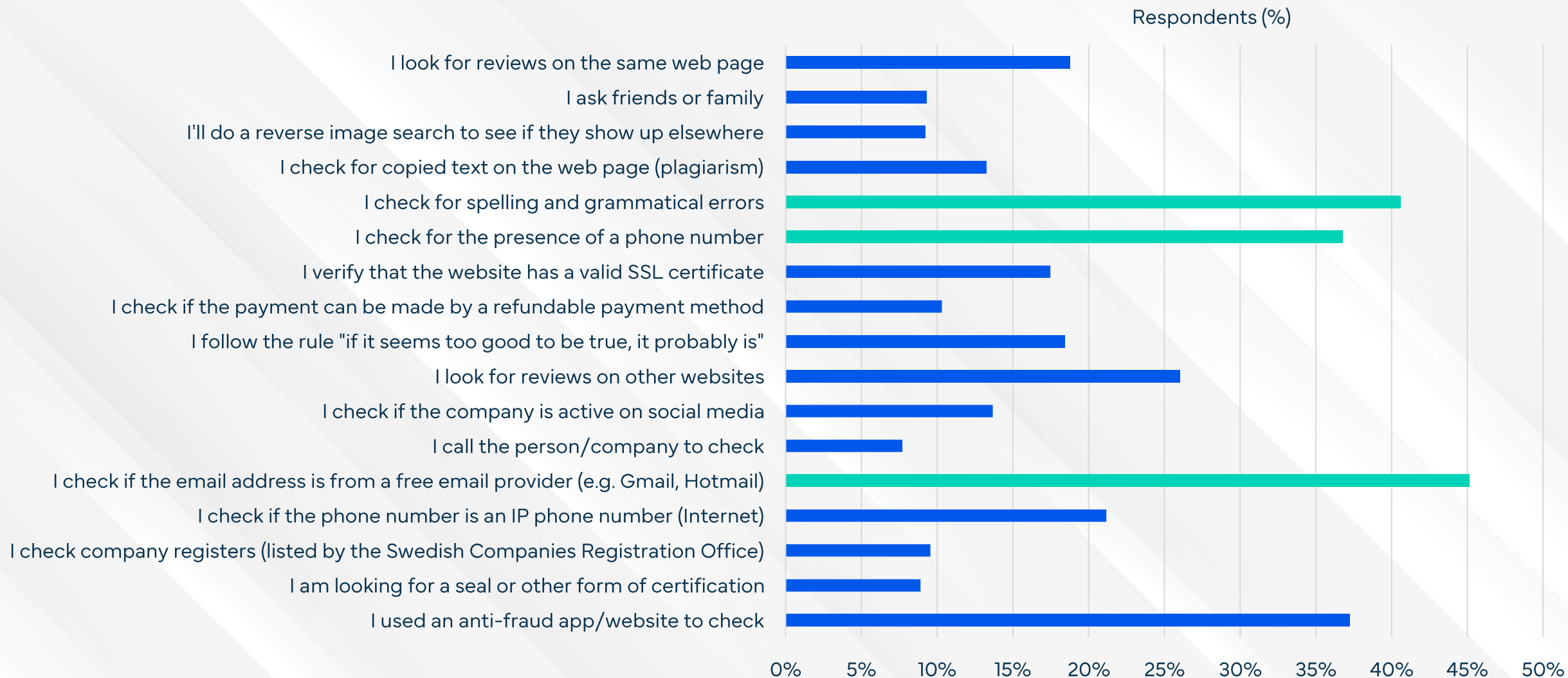
# The inability to recognize scams catches Japanese victims off guard



Several victims admitted to lacking scam awareness skills while others took the risk despite uncertainty.

Q19 - What was the main reason you were deceived?

# Japanese like to check if the email address is from a free provider

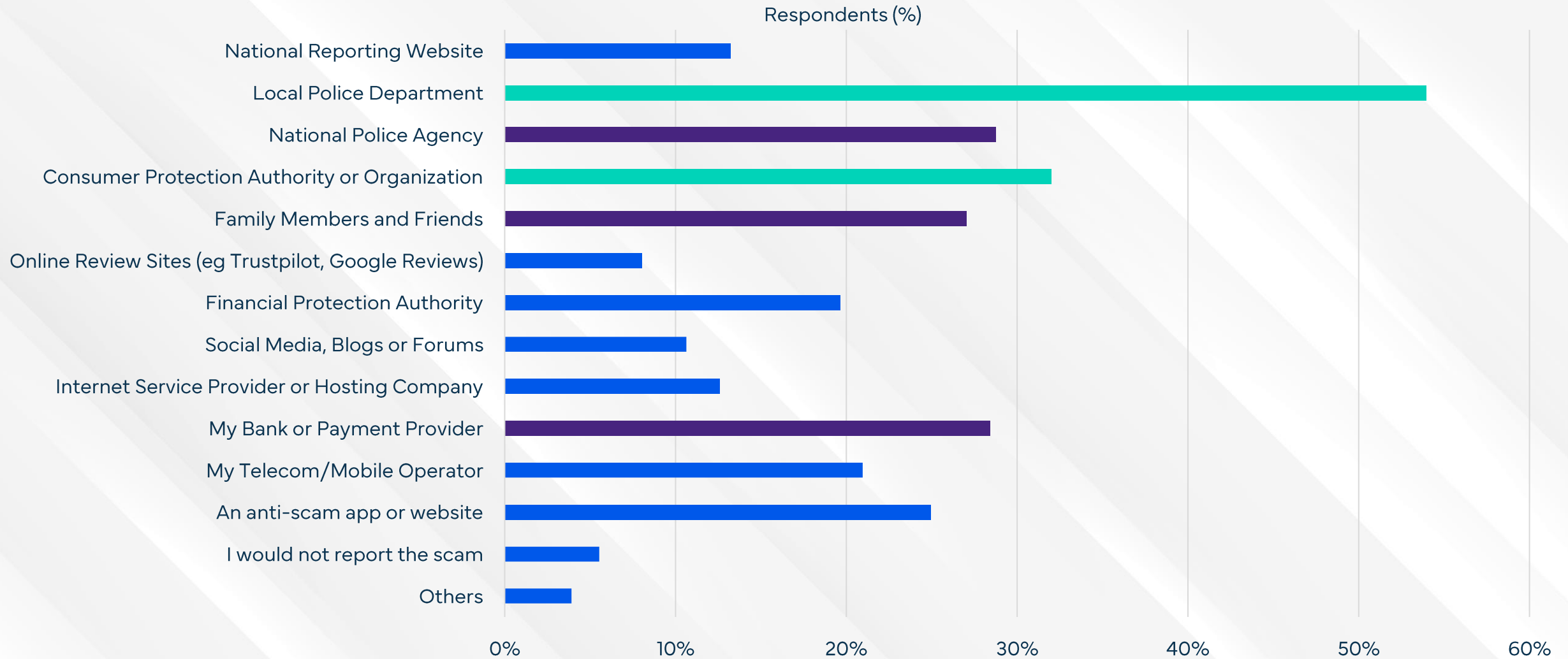


Many reported checking for spelling and grammatical errors & the presence of a phone number.

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



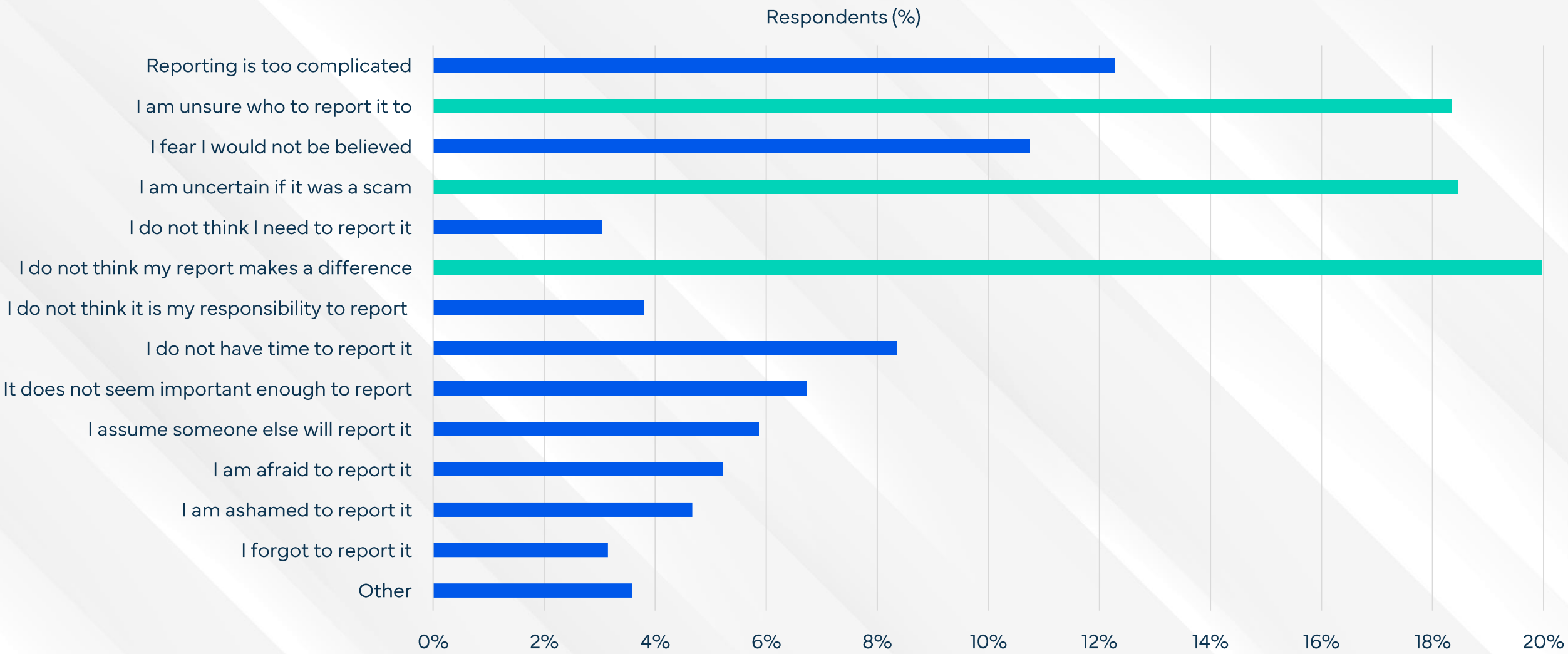
# Scams are mostly shared with local police station & consumer agencies



National police agency, banks, & family/friends are also popular places to report scams.

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

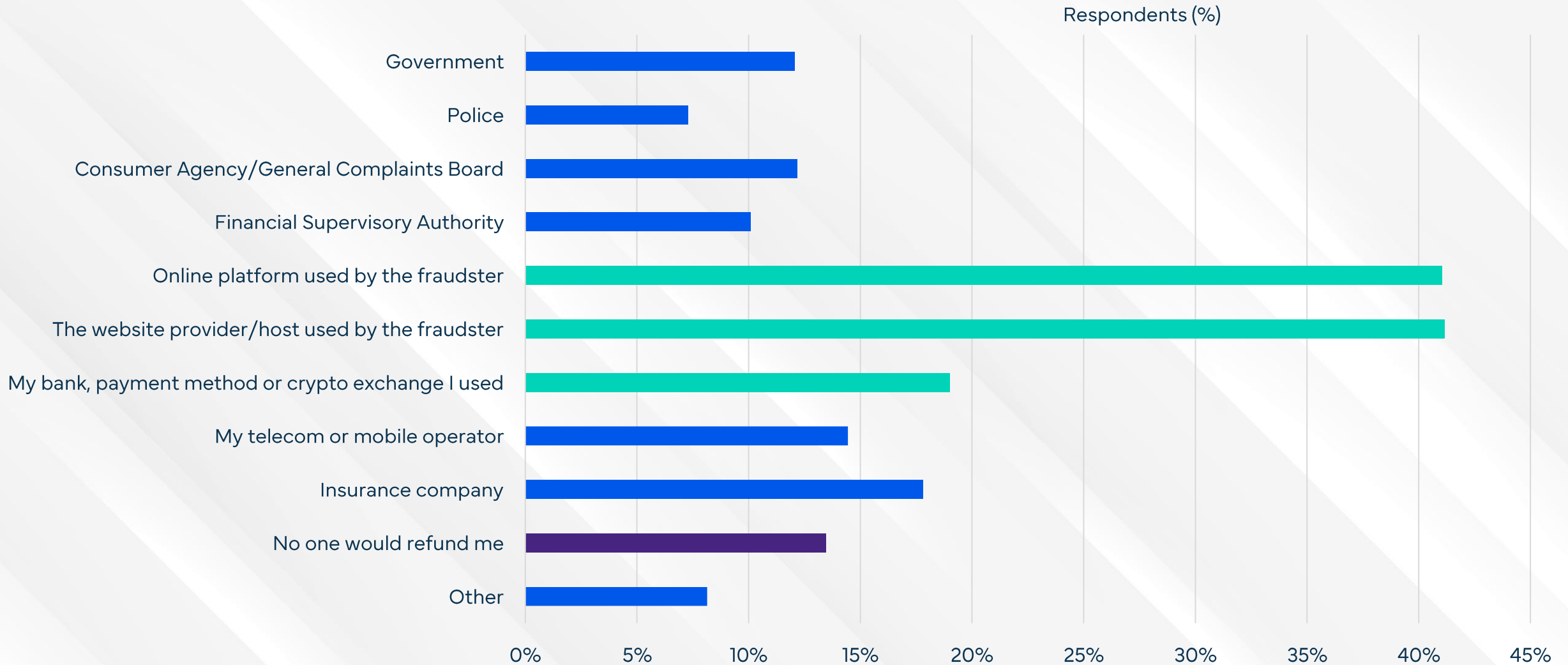
# Many Japanese don't report scams assuming it won't make a difference



Other reasons are doubts about identifying scams & uncertainty where to report them.

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

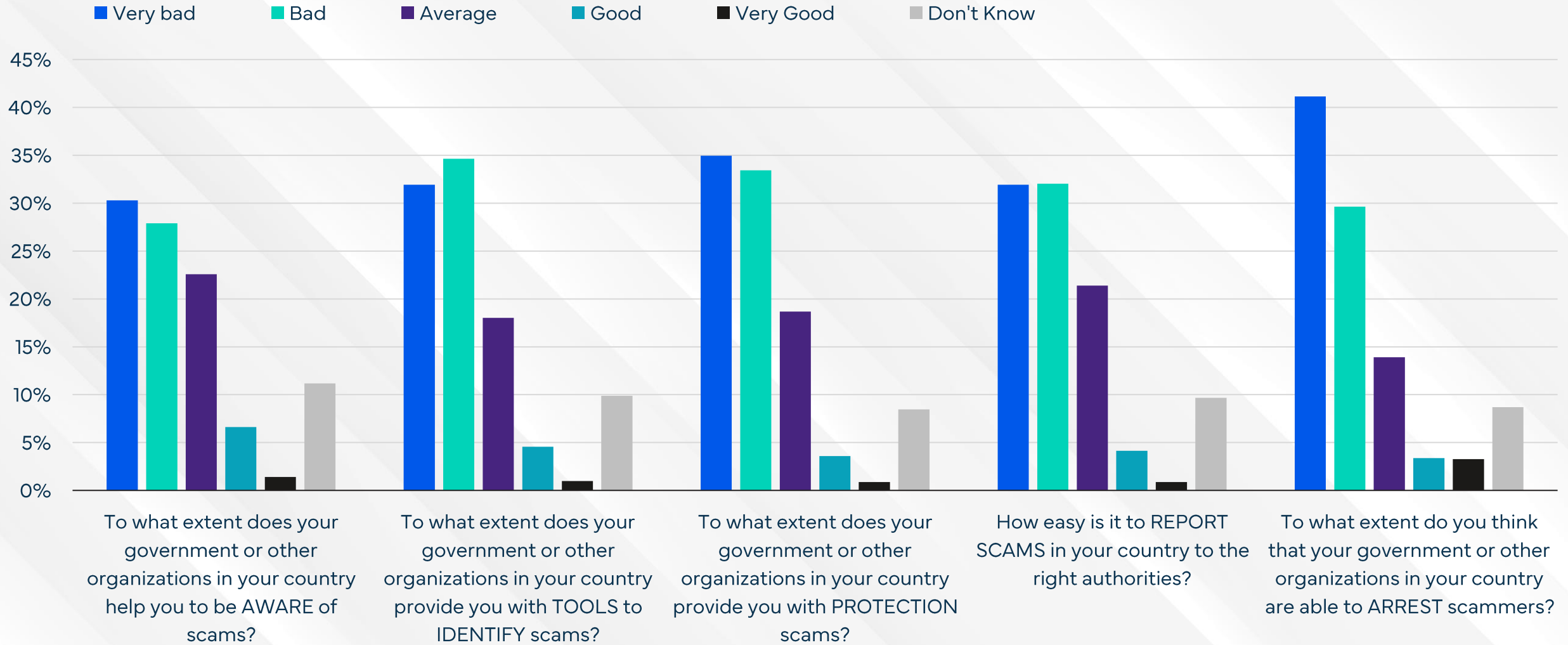
# 13% of Japanese assume no one will refund their scam losses



Others deem the website provider/host, online platform used, and bank 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?

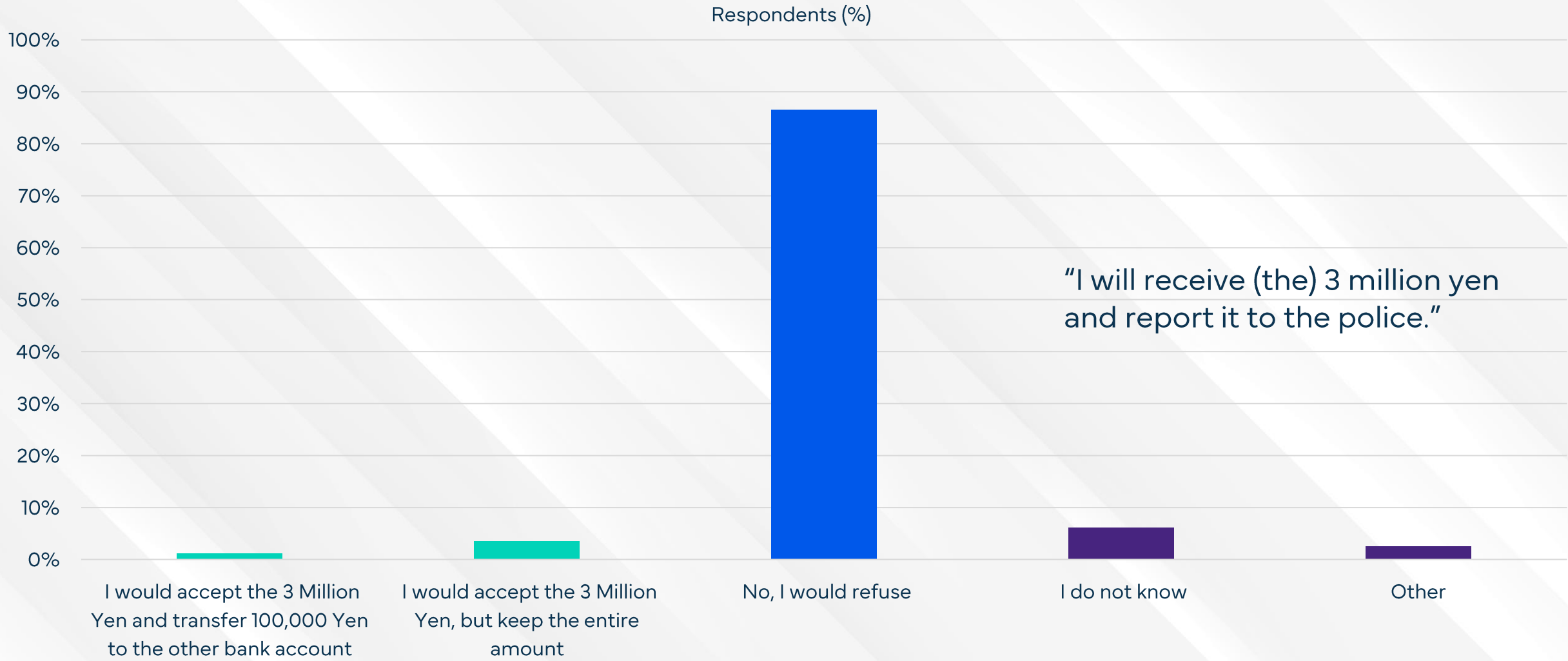
# Citizens are unsatisfied with Japan's attempts to arrest scammers



Overall, 66% of the participants rate the actions of the Japanese government as poor, 6% as satisfactory.

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?

# 1% of Japanese admit that they would consider being a money mule



However, 87% 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?

# About This Report





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.



Whoscall, powered by Gogolook, is a cutting-edge digital anti-scam tool designed to protect users from scams across various channels, including phone calls, text messages, and links. With over 100 million downloads globally, it features the most comprehensive database in East and Southeast Asia, covering more than 2.6 billion phone numbers.



ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). Our platform delivers real-time detection of suspicious activities, protecting websites, phone calls, messages, and online platforms from potential scams. With the world's largest scam database, we share insights with 400+ partners, collectively protecting more than 1 billion consumers worldwide.



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.



## 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





**whoscall**

### Disclaimer

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

It is strictly prohibited to use information published in this report without the authors' prior consent. Any violation of such rule will result in a fine of €25,000, as well as in a further penalty of €2,500 for each day that such non-compliance continues. The authors permit the use of small sections of information published in the report provided that proper citations are used (e.g., source: [www.gasa.org](http://www.gasa.org))

### Global Anti-Scam Alliance (GASA)

Oder 20 - UNIT A6311  
2491 DC The Hague  
The Netherlands

Email: [partner@gasa.org](mailto:partner@gasa.org)

X (Twitter): @ScamAlliance

LinkedIn: [linkedin.com/company/global-anti-scam-alliance](https://www.linkedin.com/company/global-anti-scam-alliance)

