SCAMADVISER

whoscall

The State of Scams in South Korea 2024

GASA
Global Anti-Scam Alliance

Scammers hit 1-in-10 South Koreans in 12 months

The 2024 State of Scams in South Korea report, an annual study conducted by the **Global Anti-Scam Alliance (GASA)** in collaboration with **Whoscall** and **ScamAdviser**, provides an in-depth look at the challenges and progress in combatting scams across the nation. With responses from **708 South Koreans**, this report highlights the evolving tactics of scammers and the pressing need for more robust scam prevention strategies.

Despite increased awareness efforts, only **47% of South Koreans reported confidence in their ability to recognize scams**, while 15% were not confident at all. Unfortunately, **79% of South Koreans encountered scams at least once per month**, a significant 13% increase compared to last year. Moreover, **59% faced more scam encounters in the last 12 months**, indicating an escalating trend in scam attempts. Although **11% experienced fewer scam encounters**, the data shows that scammers are becoming more aggressive.

Awareness of the use of artificial intelligence (AI) by scammers is high, particularly regarding AI-generated text and chat. However, there is still a lack of knowledge about more complex AI applications, such as images and videos, which could leave many vulnerable to advanced scam tactics. The **majority of scams are delivered through text/SMS messages or phone calls**, with a **5% increase in SMS-based scams since 2023**. Platforms like Instagram, KakaoTalk, and Naver Email are frequently exploited, with Facebook scams continuing to rise as well.

Scam underreporting remains a significant issue, with **82% of South Koreans not reporting scams to law enforcement**—a worrying 16% increase from the previous year. Only **14% of respondents stated they reported the scam to law enforcement or another authority**. The most common reasons for not reporting include the perception that the process is too complex and the belief that reporting will not lead to the recovery of lost funds.

Investment and identity theft remain the most prevalent types of scams in South Korea, with many respondents falling victim to scams involving impersonation on platforms like KakaoTalk, remote work opportunities promising high returns, and romance scams. Alarmingly, **41% of scams are completed within 24 hours of first contact**, and 24% are over within minutes, demonstrating the speed and efficiency with which scammers operate.

The average loss per victim was $2,738, and **only 8% of victims were able to fully recover their losses**, reflecting a slight increase in recovery rates. However, the majority (62%) of those who tried to recover their funds were unsuccessful, contributing to the heavy emotional toll that scams have taken, with **59% of victims reporting a strong emotional impact**—a 7% rise compared to last year.

Trust in the internet has also eroded, with **62% of South Koreans expressing less trust in online activities** due to scams. Many victims reported that they were caught off guard by offers that seemed too good to be true or acted hastily without taking the time to verify legitimacy. Although **40% of respondents follow the "if it seems too good to be true, it probably is" rule**, this caution has not been enough to stem the tide of scams.

Citizens remain dissatisfied with government efforts to combat scammers, with 54% rating these efforts as very poor and only 14% expressing satisfaction. South Koreans need greater support from government authorities, financial institutions, and digital platforms to ensure more effective protection against scams. With a rising number of incidents and billions lost, it is crucial that South Korea strengthens its public awareness initiatives, simplifies reporting processes, and improves law enforcement action to tackle the growing threat of scams effectively.

Jorij Abraham
Managing Director

GASA
Global Anti-Scam Alliance

Sam Rogers
Director of Marketing

Navigating the Rising Tide of Scams in South Korea: Insights and Solutions

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 South Korea.

How significant has the issue of scams become in South Korea?

This report shows that scams have escalated in both frequency and complexity, with 79% of South Koreans encountering scam attempts at least once per month—a significant 13% increase from 2023. The rise of AI has also influenced the scam landscape, with 40% of South Koreans uncertain whether AI was used in scams against them. Despite the growing threat, 82% of scam victims in South Korea did not report their experiences to law enforcement, highlighting a gap in the response to these scams.

What types of scams have trended in South Korea recently?

In South Korea, scam trends have evolved with various tactics being primarily delivered through digital channels such as text messages, phone calls, emails, and social media platforms. Among these, KakaoTalk, Instagram, and Naver Email are the most frequently exploited platforms. Scammers are increasingly utilizing these platforms to target victims through phishing, impersonation, and deceitful schemes. Investment scams and identity theft remain the most common types of scam in South Korea. Scammers share stolen personal information for financial fraud or impersonation, making it essential for individuals to detect and safeguard their personal data.

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

To enhance education and anti-scam efforts, South Korea’s police agencies and the Financial Supervisory Service have partnered with well-known trust technology companies. These collaborations aim to raise public awareness of scam prevention while leveraging advanced technologies to improve scam detection and prevention, ensuring the safety of South Korean citizens in the digital environment.

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

Although many Koreans now use anti-scam apps or websites to verify offers, most remain dissatisfied with the efforts of the government and corporations to combat scams. There is a clear need for more proactive measures. Simplifying the reporting process through a centralized platform could encourage more victims to come forward, while stronger collaboration between the government, chaebols, and tech companies could enhance scam detection and recovery. Expanding AI-driven detection and integrating scam prevention features into digital services would also help bolster consumer protection.

Aaron Chiou
Product Director

Defining Digital Defense: Whoscall's Approach to Curbing the Scam Epidemic in South Korea

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 Korea 2024 State of Scams report, GASA interviewed Manwoo Joo, COO of Gogolook, to share insights on the in-depth analysis of the evolving scam landscape in South Korea, to equip consumers with the knowledge and tools they need to stay one step ahead of scammers.

How big has the problem of scams become in Korea? In the first half of this year, the number of scam cases reported to the prosecution increased by 10% compared to the same period last year. Experts have analyzed that there has been a sharp rise in social network service (SNS) scams using platforms such as Telegram and Naver Band.

According to the report from Supreme Prosecutors' Office Republic of Korea in September, the number of scam cases reported from January to June 2024 reached 117,919. This represents a 10% increase compared to 107,168 cases in the first half of 2023.

The number of scam cases has steadily increased over the past three years. In the first half of 2021 and 2022, there were 93,005 and 93,566 cases, respectively. This means that over the past three years, the number of scam cases has increased by 26.8%.

Which scams have been trending in Korea over the past? The most common scam schemes in Korea in the first half of 2024 include online job scams, government account hijacking, deepfake and AI scams, P2P payment scams, and parcel delivery scams. Experts have noted a rise in these scams on platforms like Telegram, Naver Band, and KakaoTalk, affecting all age groups. Popular scams such as stock trading guidance and romance scams have emerged, especially as older users increasingly join these platforms.

Which actions have been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn? South Korea has taken several measures to combat the rising tide of scams, focusing on strengthening legal frameworks, increasing public awareness, and utilizing technology to prevent scam.

1. National Police Agency develops an app for blocking and deleting malicious apps: Citizen Konan (시티즌코난) is an AI-based mobile application for phishing detection and prevention, developed by the Korean National Police Agency and Infiniguru in 2021. With over 1 million downloads, this app monitors user devices 24/7 to detect and block malicious apps in real-time. It specializes in identifying phone interception apps used for voice phishing, as well as apps that impersonate financial institutions, public institutions like the police and prosecutors, medical services, couriers, shopping platforms, and malicious body camera apps. Through this approach, Citizen Konan ensures comprehensive protection against phone-based financial fraud.

2. The Financial Services Commission, a government agency, implements "Safe Blocking," a protection service for financial transactions. The regulation can block all new credit transactions that may occur without our knowledge in advance. Financial users living in rural areas can easily apply for and use the Safe Blocking service, which will be extended not only to banks but also to agricultural cooperatives, fisheries cooperatives, community credit cooperatives, and post offices. Proxy applications (through authorized representatives) and non-face-to-face applications for the elderly and those who have difficulty visiting branches will also be considered.

Other regions and organizations can benefit from adopting similar measures, especially by leveraging AI, strengthening legal frameworks, and boosting public awareness through educational campaigns.

What further actions could give consumers the upper hand in fighting scams? Most Koreans are aware of the risks associated with voice phishing and smishing scams, but there is a lack of understanding about preventive measures and response strategies. It is hoped that there will be increased promotion of anti-scam policies and apps like Whoscall or Citizen Konan to better educate the public and prevent scams.

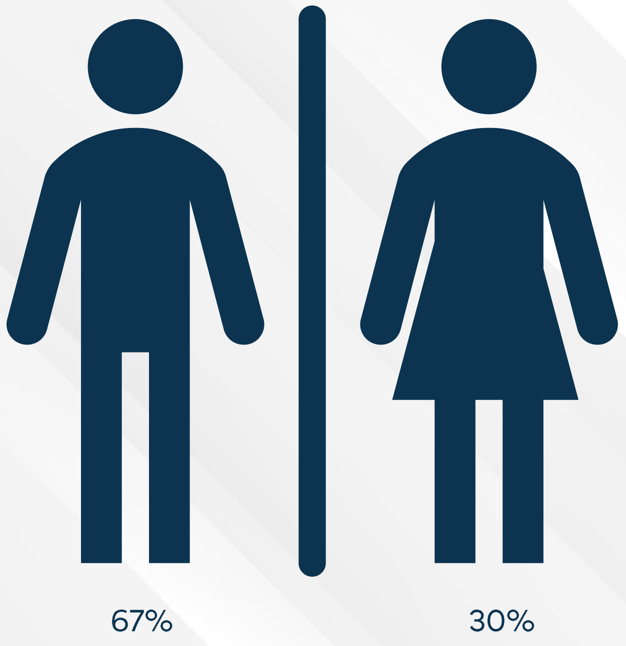
Manwoo Joo
COO
Gogolook

Gogolook

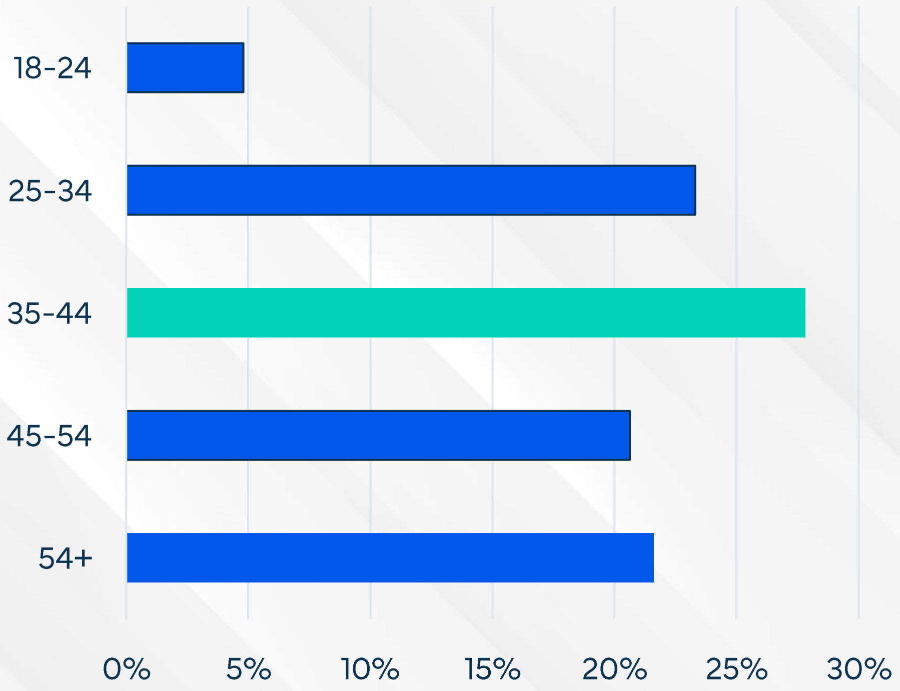
708 South Koreans completed the State of Scams survey

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

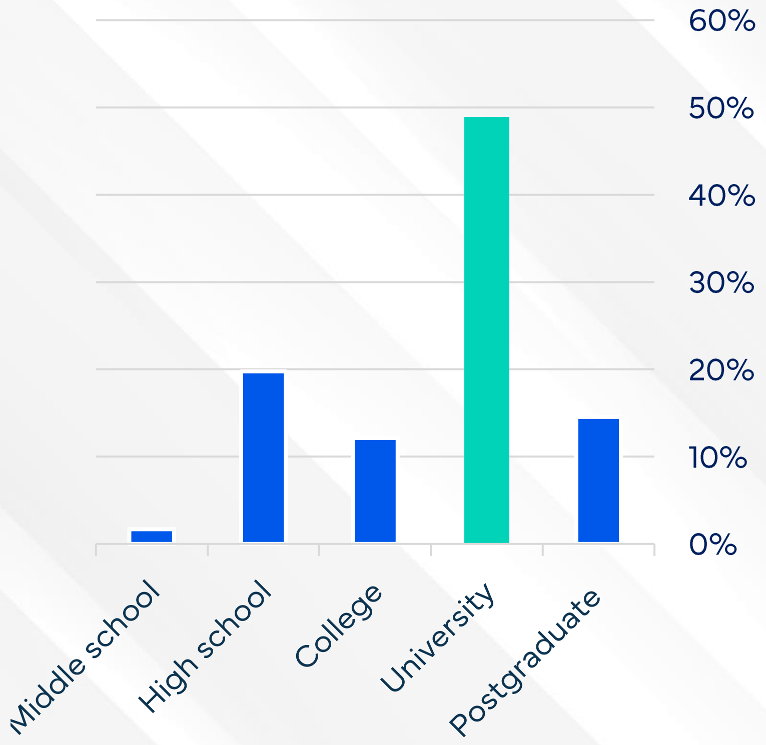
Gender



Age Range

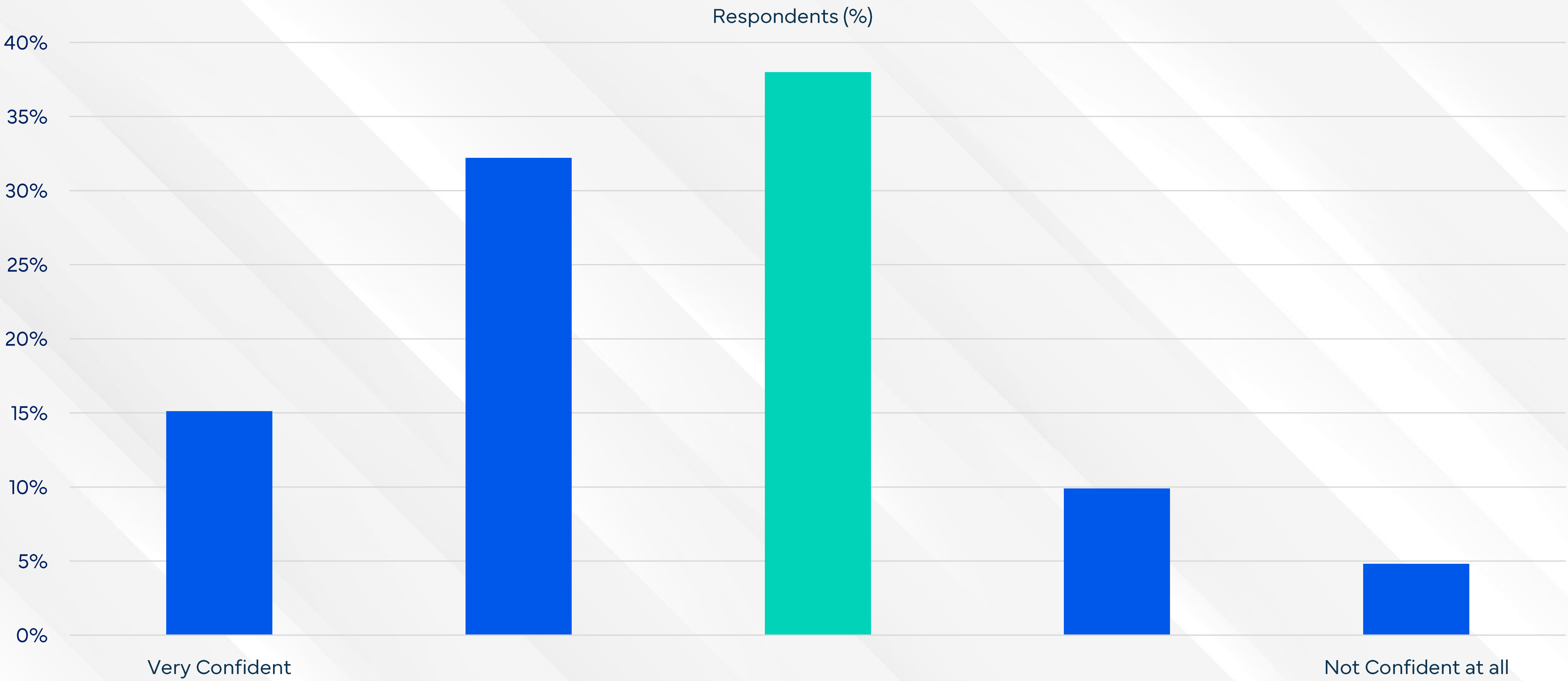


Education



The demography of respondents to the State of Scams in the South Korea 2024 survey consists of more men than women. A large proportion were between 35-44 of age with a university education.

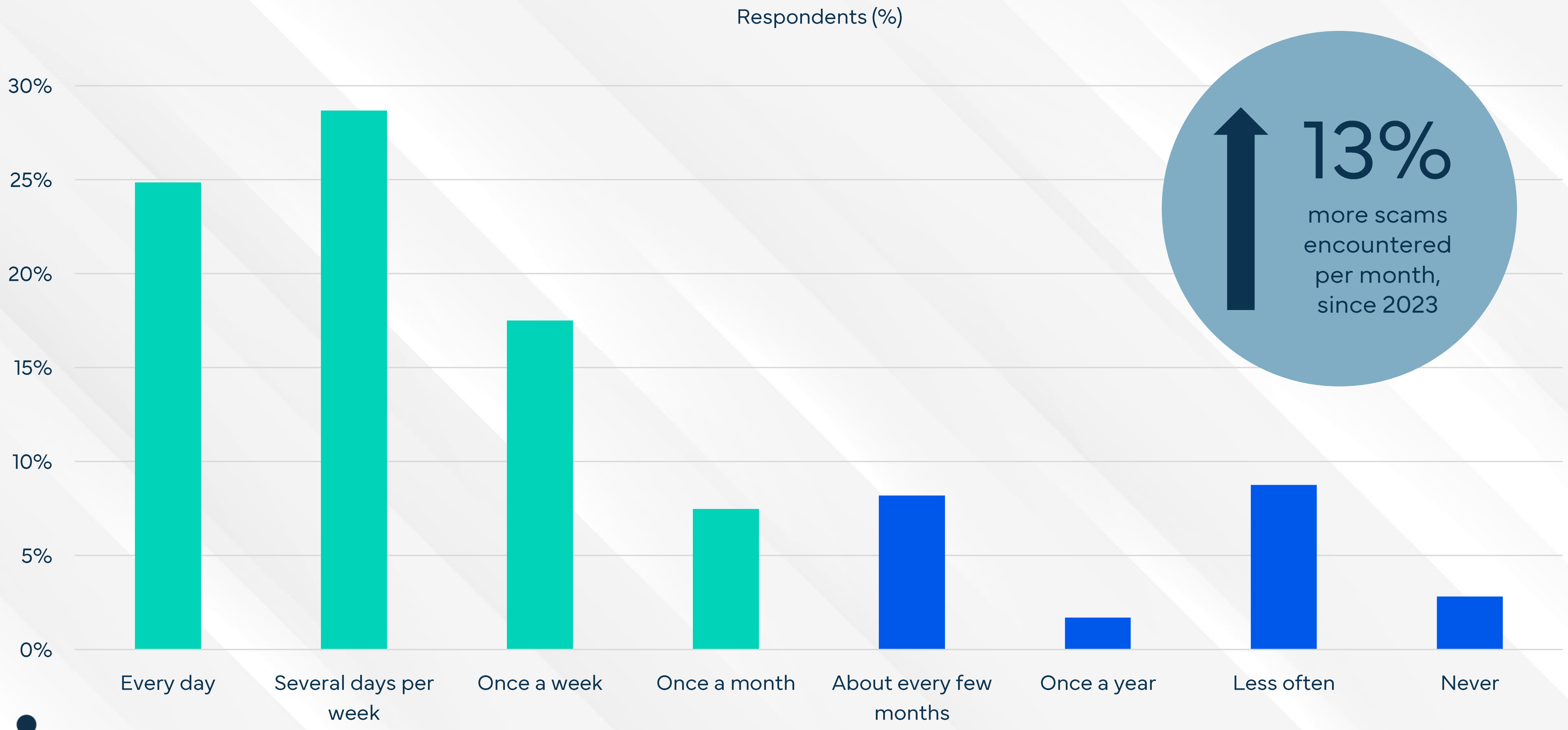
47% of South Koreans are confident in their ability to recognize scams



Only 15% of respondents are not (very) confident in recognizing scams, at all.

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

79% of South Korean encounter scams at least once per month



13% more scams encountered per month, since 2023

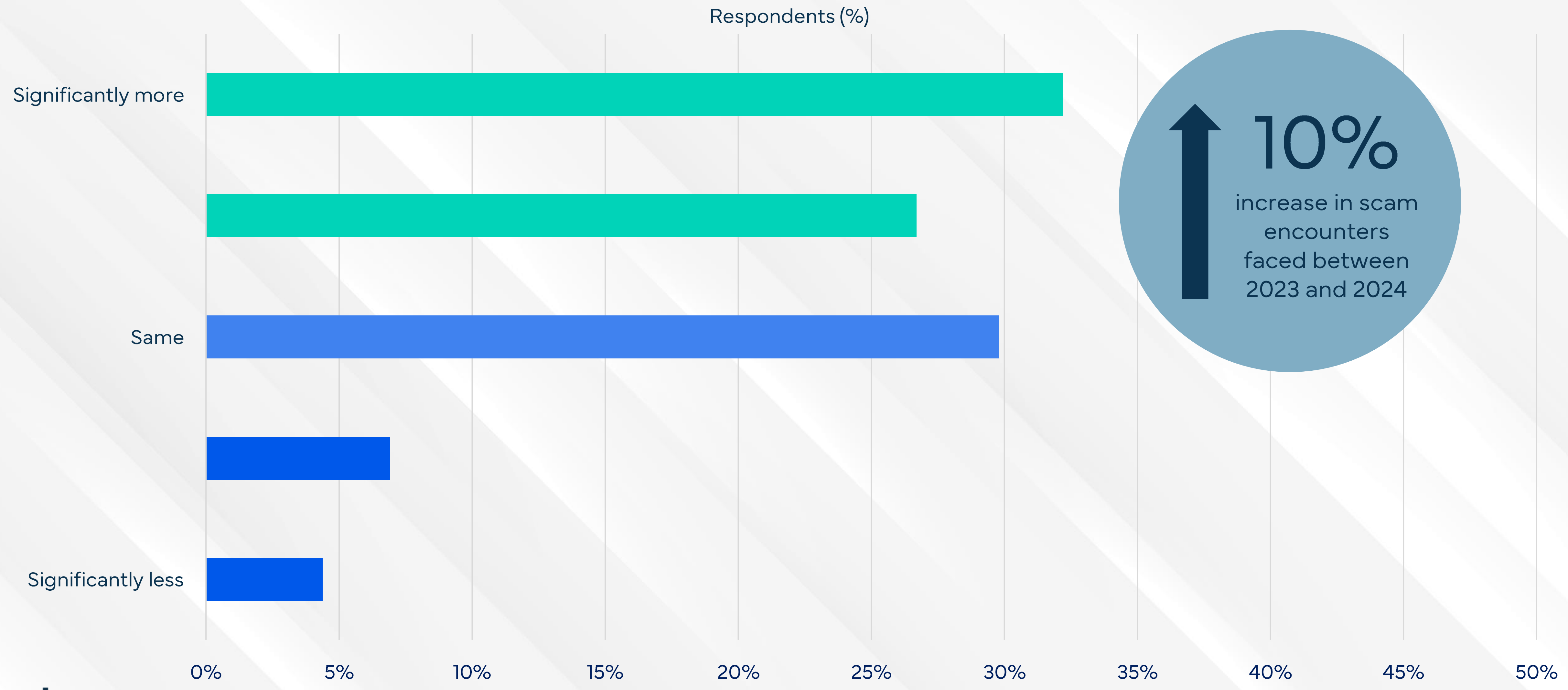
10% of South Koreans respondents admitted to rarely facing scams in the previous 12 months.

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.

59% of South Koreans faced more scam encounters in the last 12 months

SCAMADVISER whoscall

GASA Global Anti-Scam Alliance



10%

increase in scam encounters faced between 2023 and 2024

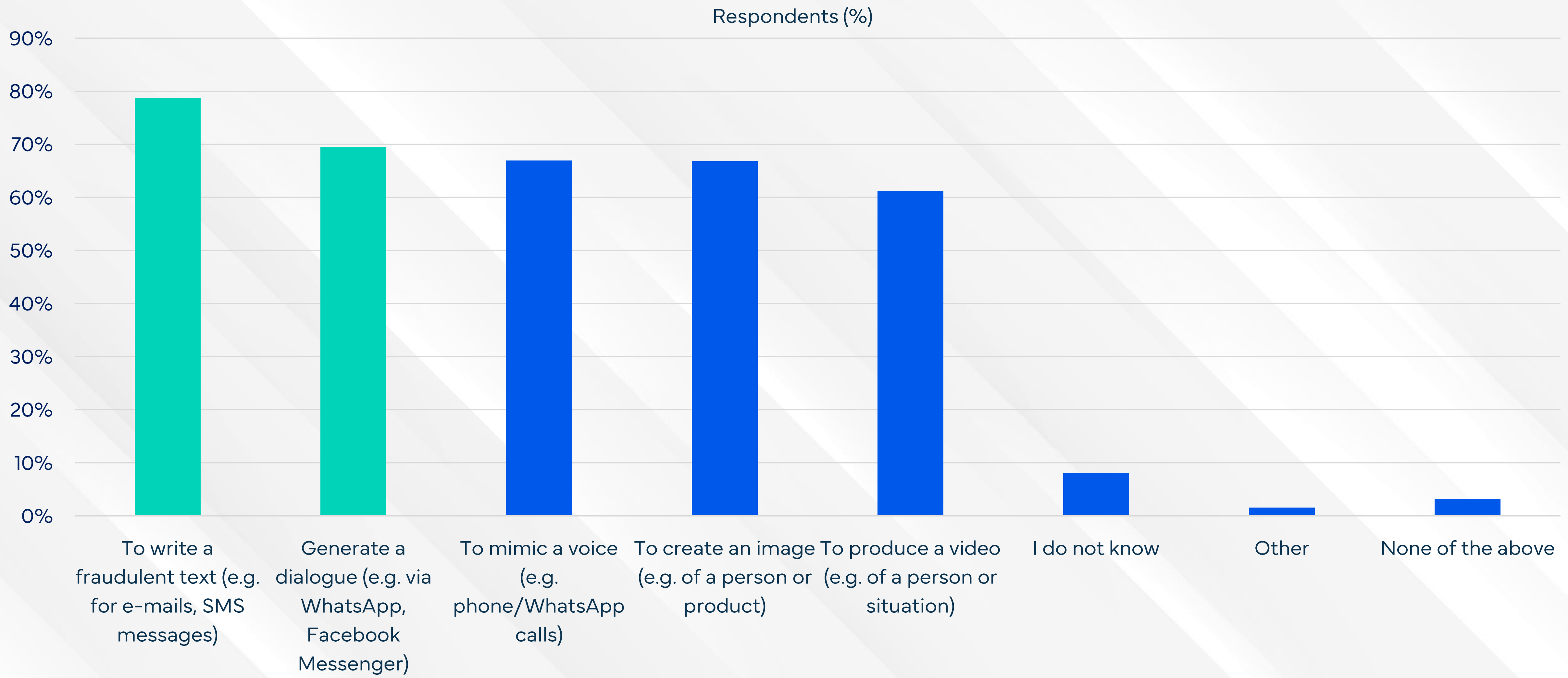
11% of South Korean respondents experienced a reduction in scam encounters in the past 12 months.

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 South Korean are aware scammers can use AI against them

SCAMADVISER whoscall

GASA Global Anti-Scam Alliance

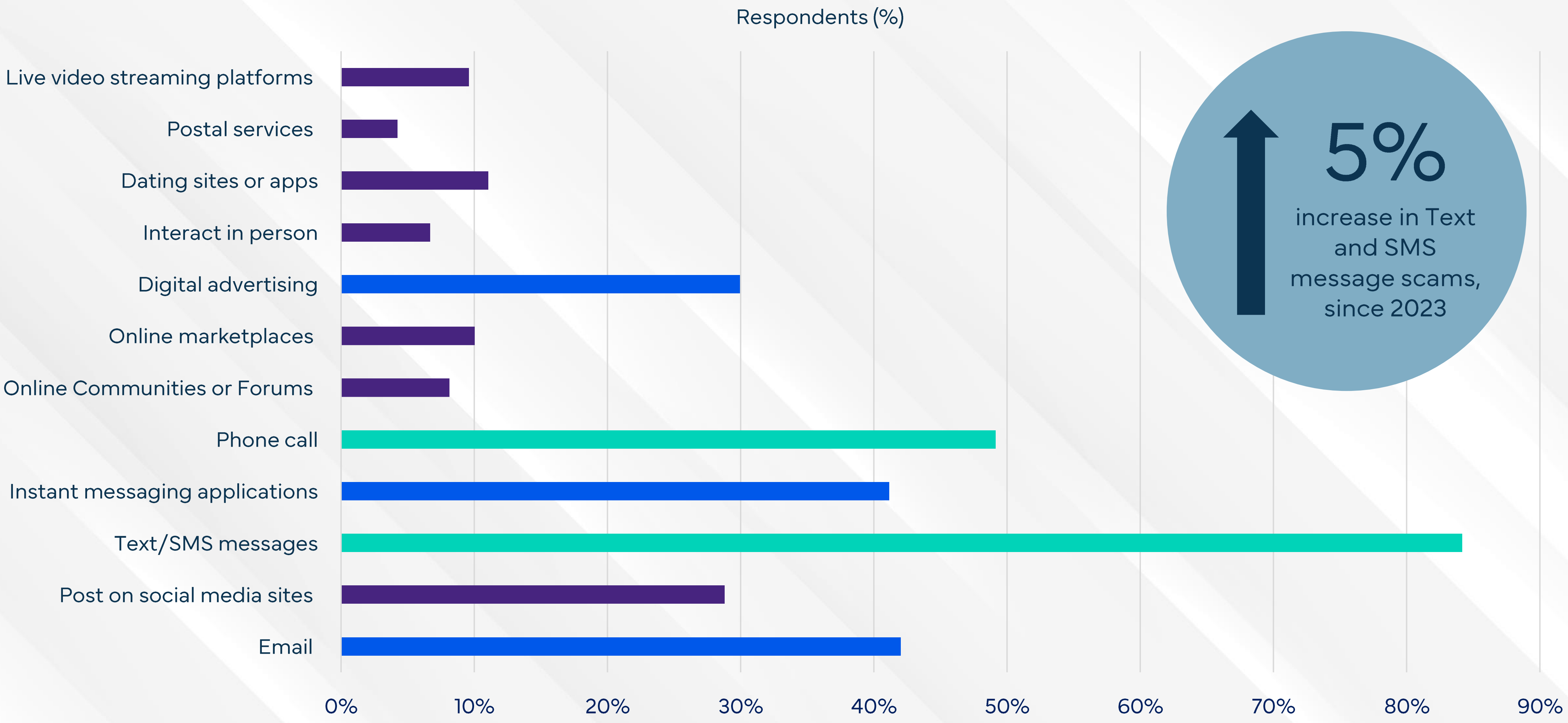


Awareness of AI generated text & chat is high, while complex images & videos are less widely known.

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

Majority of scams are delivered via text/SMS messages or phone calls

SCAMADVISER whoscall GASA Global Anti-Scam Alliance



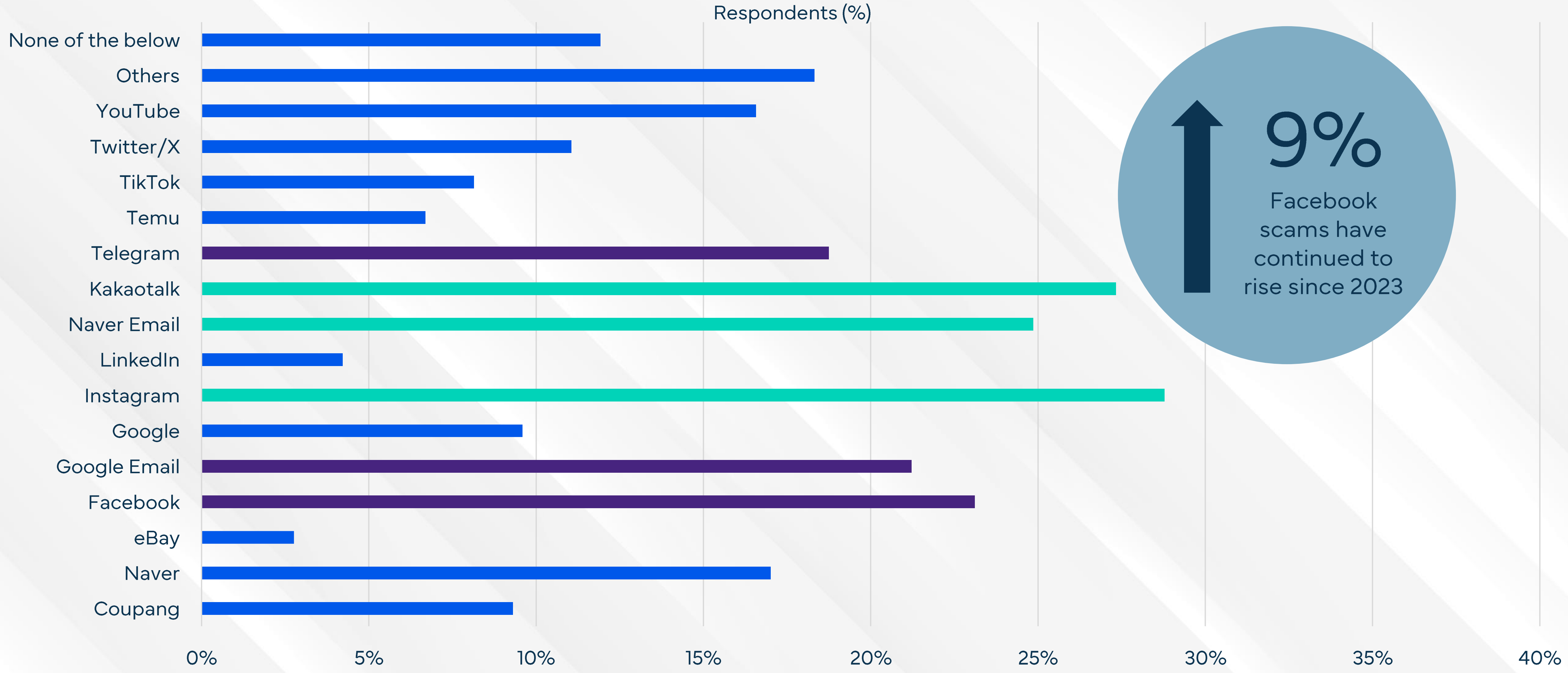
5% increase in Text and SMS message scams, since 2023

Emails, instant messaging apps, and digital advertising are also common scam media.

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

Instagram, Kakaotalk, & Naver Email are the most exploited platforms

SCAMADVISER whoscall GASA Global Anti-Scam Alliance



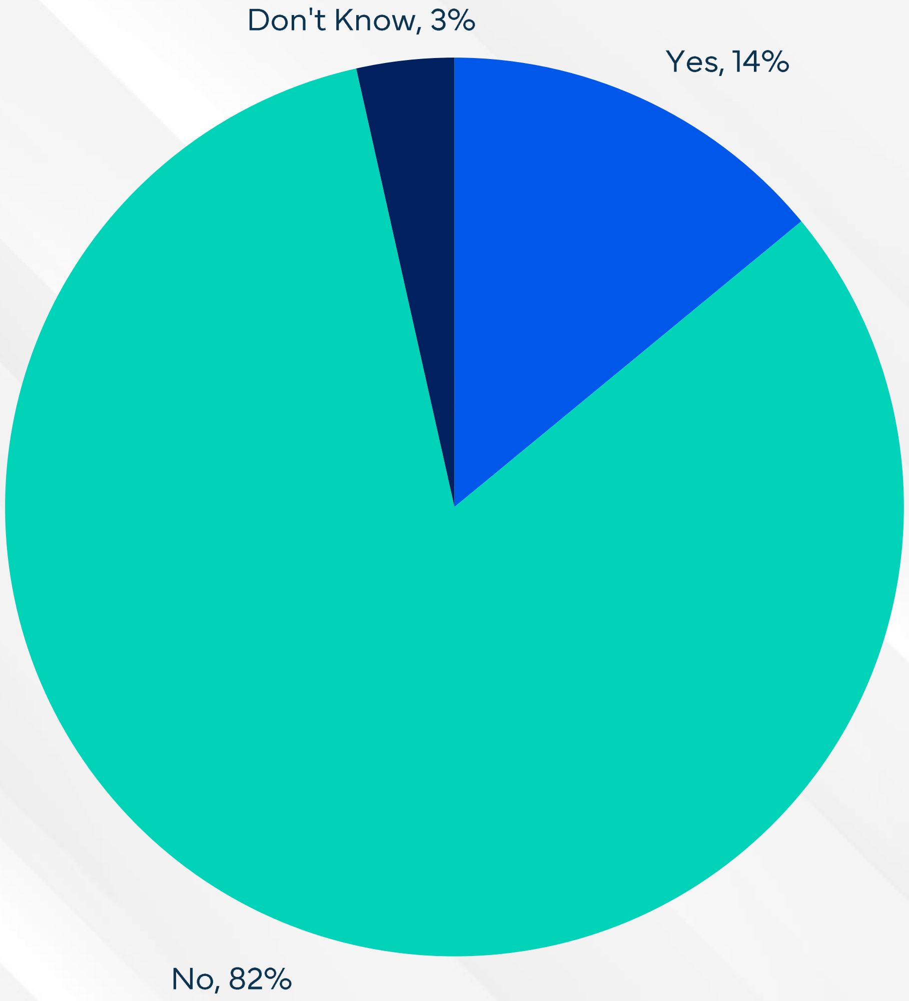
9%

Facebook scams have continued to rise since 2023

Facebook, Gmail & Telegram round out the top five platforms where people encounter scams.

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

82% of South Koreans did not report the scam to law enforcement



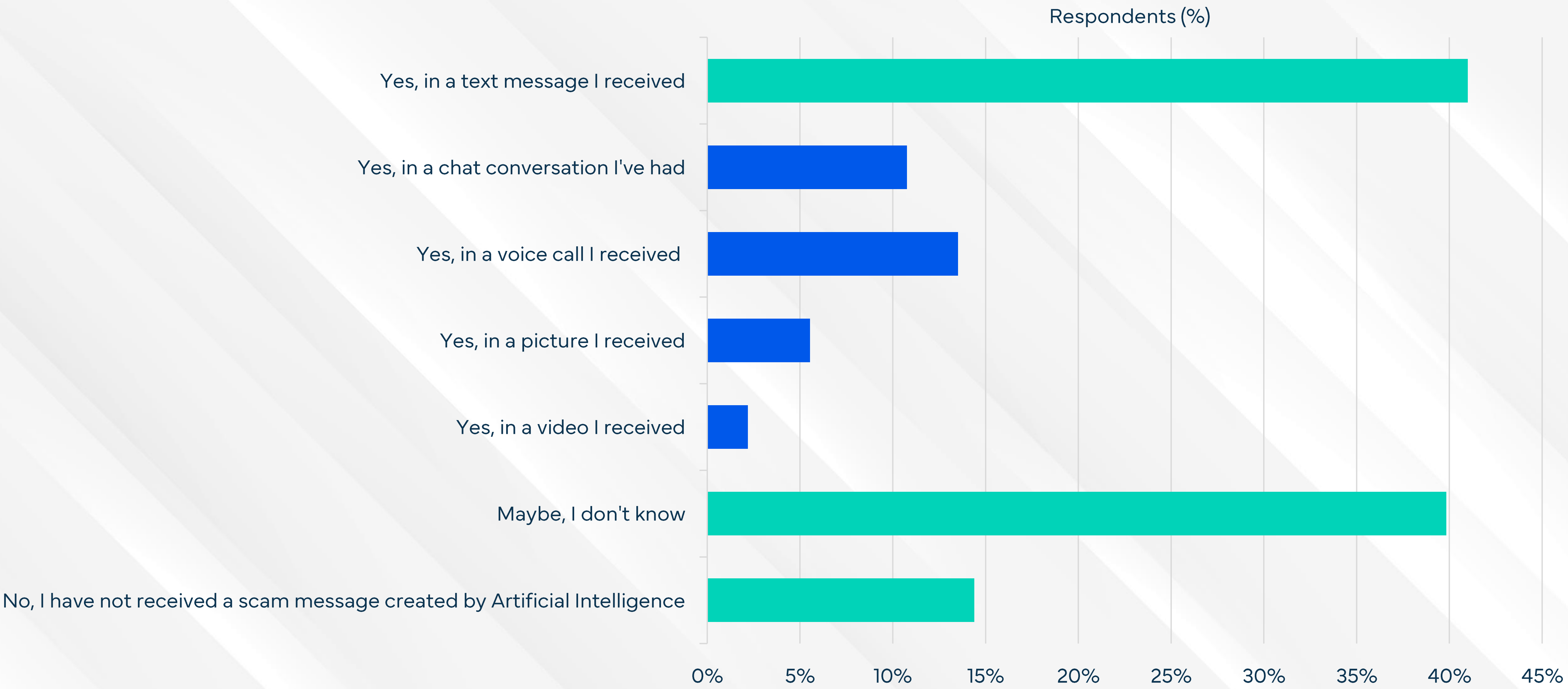
16%

increase in Koreans not reporting scams

14% 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?

40% of South Koreans were uncertain whether AI was used to scam them

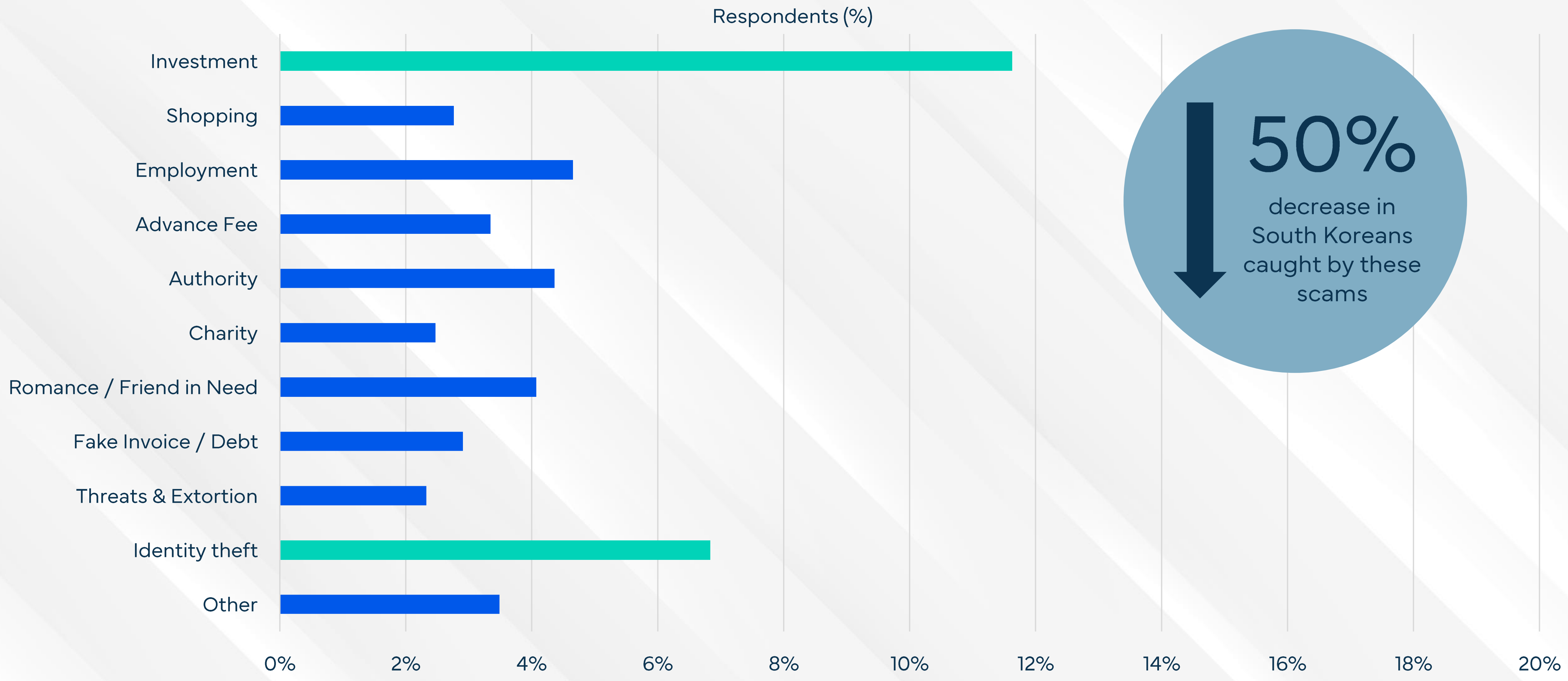


14% of South Koreans stated they did not believe they were subjected to scams utilizing AI.

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

Investment and Identity Theft remain most prevalent in South Korea

SCAMADVISER whoscall GASA Global Anti-Scam Alliance



50% decrease in South Koreans caught by these scams

73% did not fall victim to the most common scams in the last year. 0.5 scams were reported per victim.

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

South Korean scam victims share their stories

“Using KakaoTalk phishing, they impersonated my ID on my mother's phone and stole my profile picture. They approached my mother while imitating my voice on KakaoTalk and asked her to send 6 million won. Fortunately, the deposit was not made to a fake account, so there was no damage.”

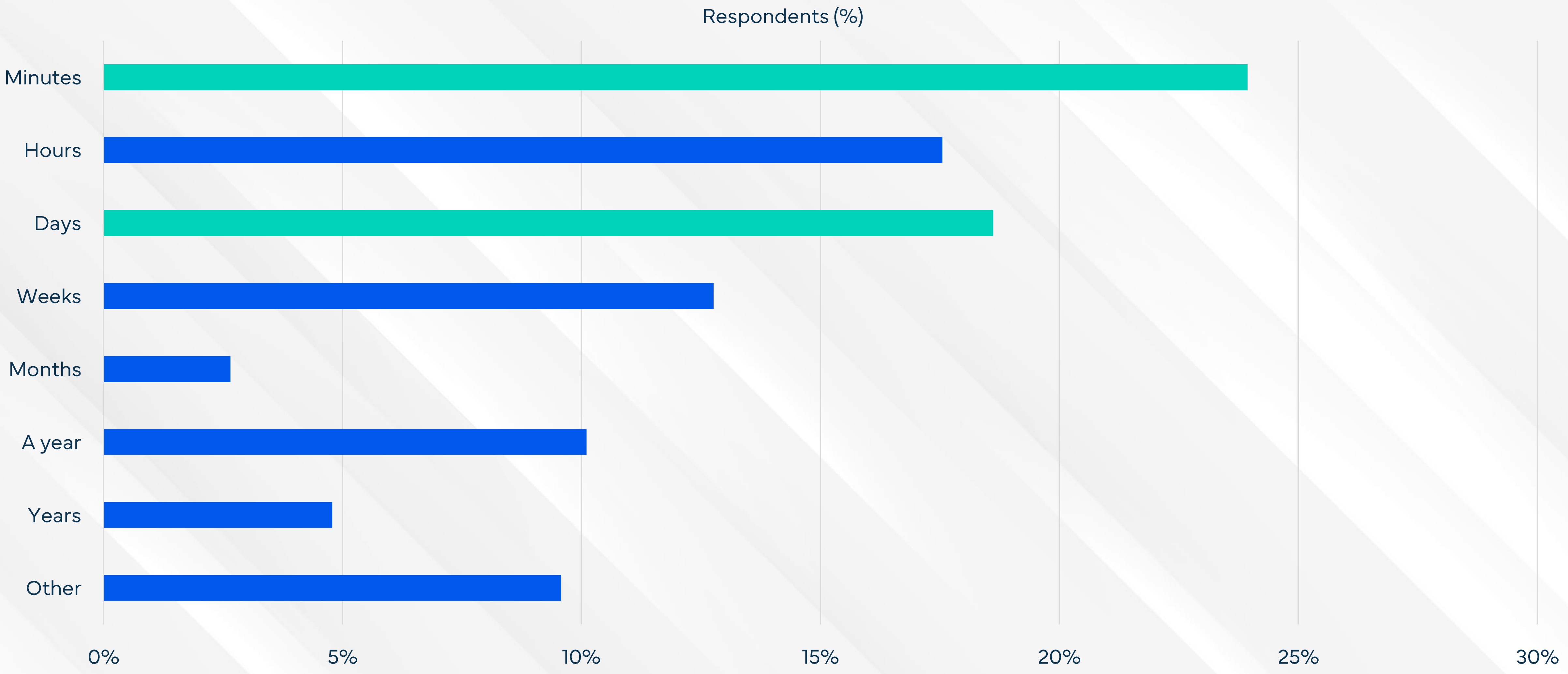
“I checked the usage history of my credit card and found that it was used overseas, so I took out overseas-related documents to prevent withdrawals.”

“I was scammed by a remote team mission. I received a text message on my phone, and it said that I could (work) anywhere, anytime, as long as I had a cell phone, and that it would take 2–3 hours of work with guaranteed high income. I bought shares that promised immediate profit returns, but after (investing), there are several fees that need to be paid even though I was initially promised only a one-time fee.”

“Pretending to be a woman overseas and approaching someone through text messages as if they were lovers (Example: I'm at Incheon Airport. When are you coming to pick me up?)”

41% of scams are completed within 24 hours of first contact

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

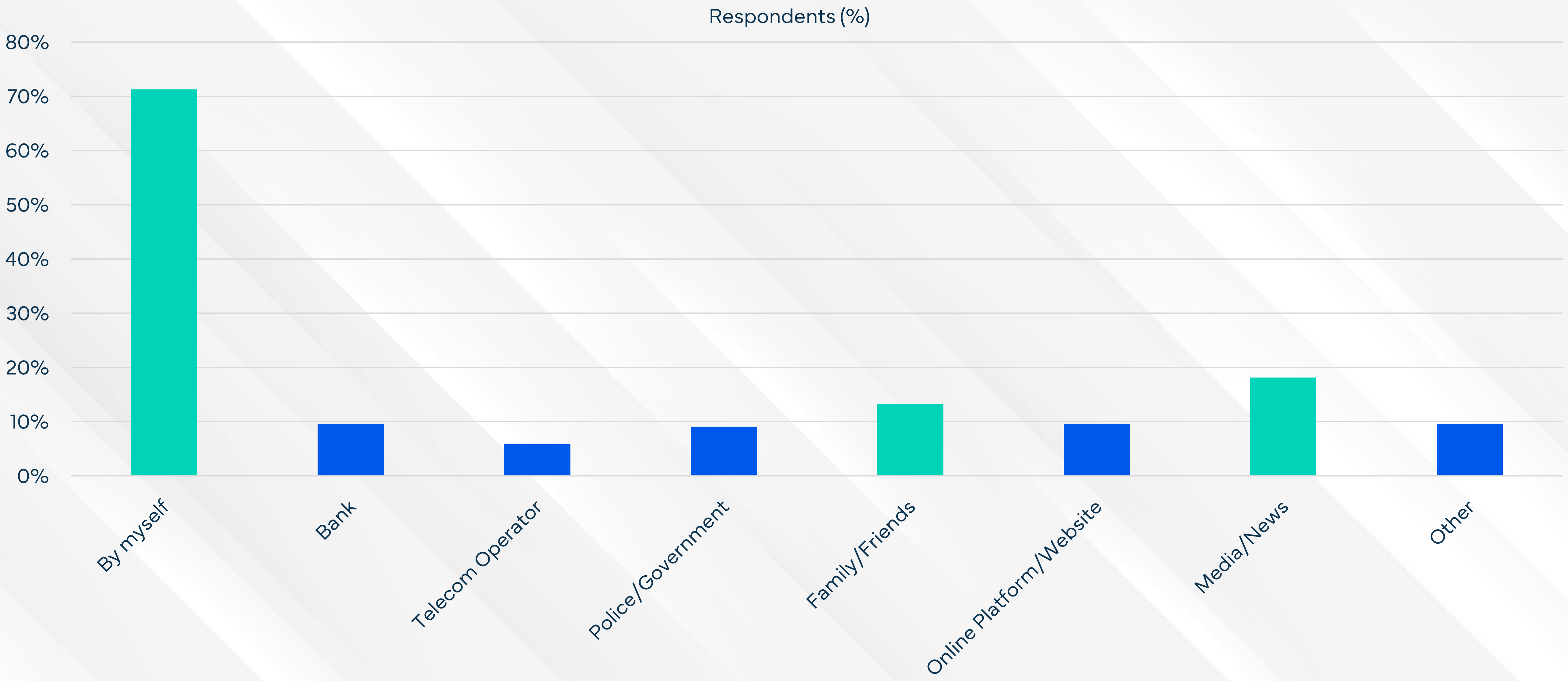


24% reported scams that were over in minutes, while 7% were scammed over a year or more.

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?

71% concluded that they had been scammed without external advice

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

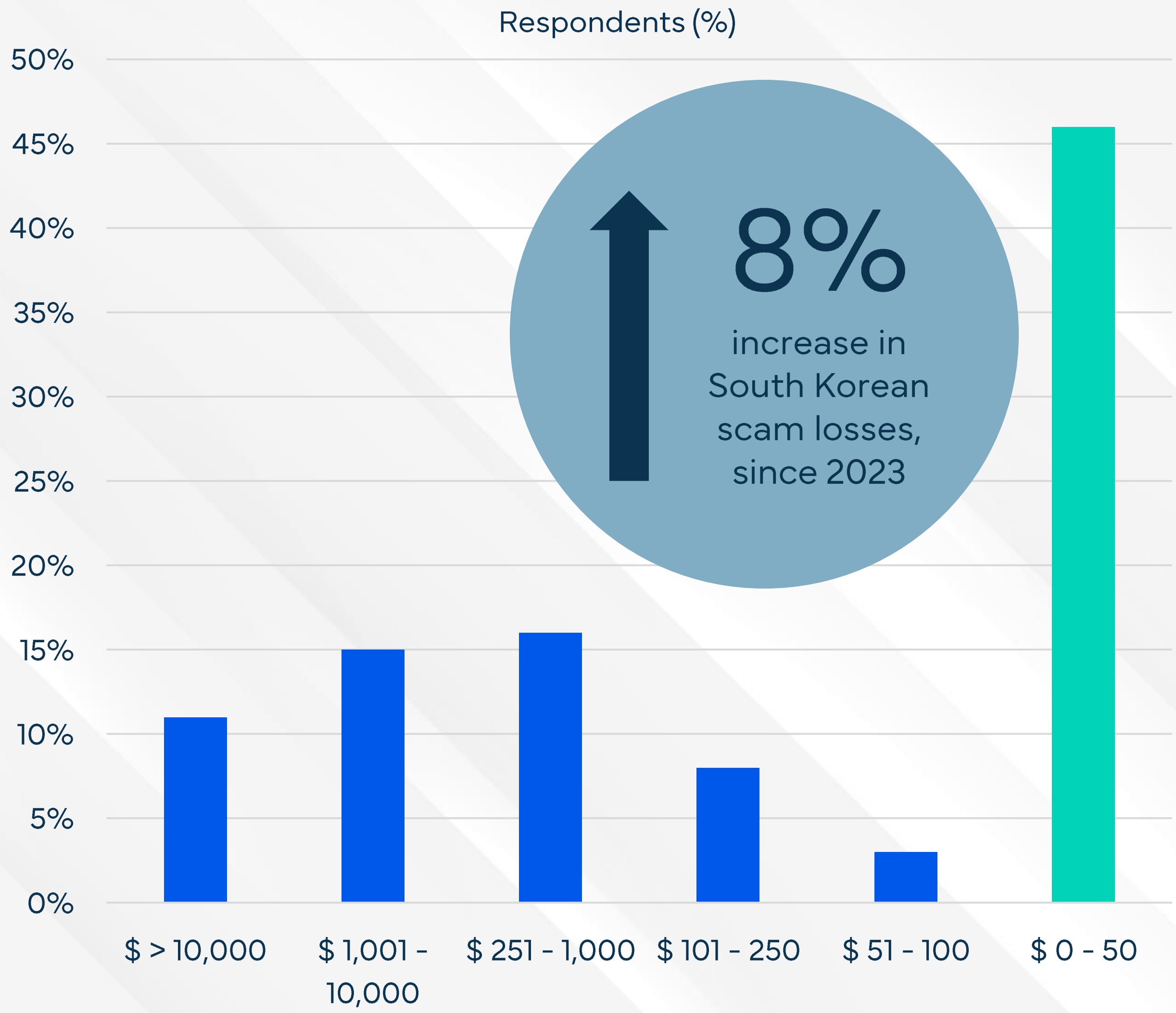


Nearly 1-in-5 victims are informed by media/news while others were enlightened by family & friends.

Q13 How did you discover you were scammed?

In total, 10% of South Korean survey participants lost money in a scam

Survey Key Statistics	
Persons approached	708
Participants losing money	69
% losing money / survey participants	10%
Average amount lost in US Dollars	2,738
Total country population	52,081,799
Population over 18 years	44,800,949
# of people scammed > 18 years	4,366,194
Estimated total scam losses (USD)	11,954,639,671
Estimated total scam losses (SKW)	16,133,728,348,131
Gross Domestic Product (USD, millions)	1,709,232
% of GDP lost in scams	0.7%



8%

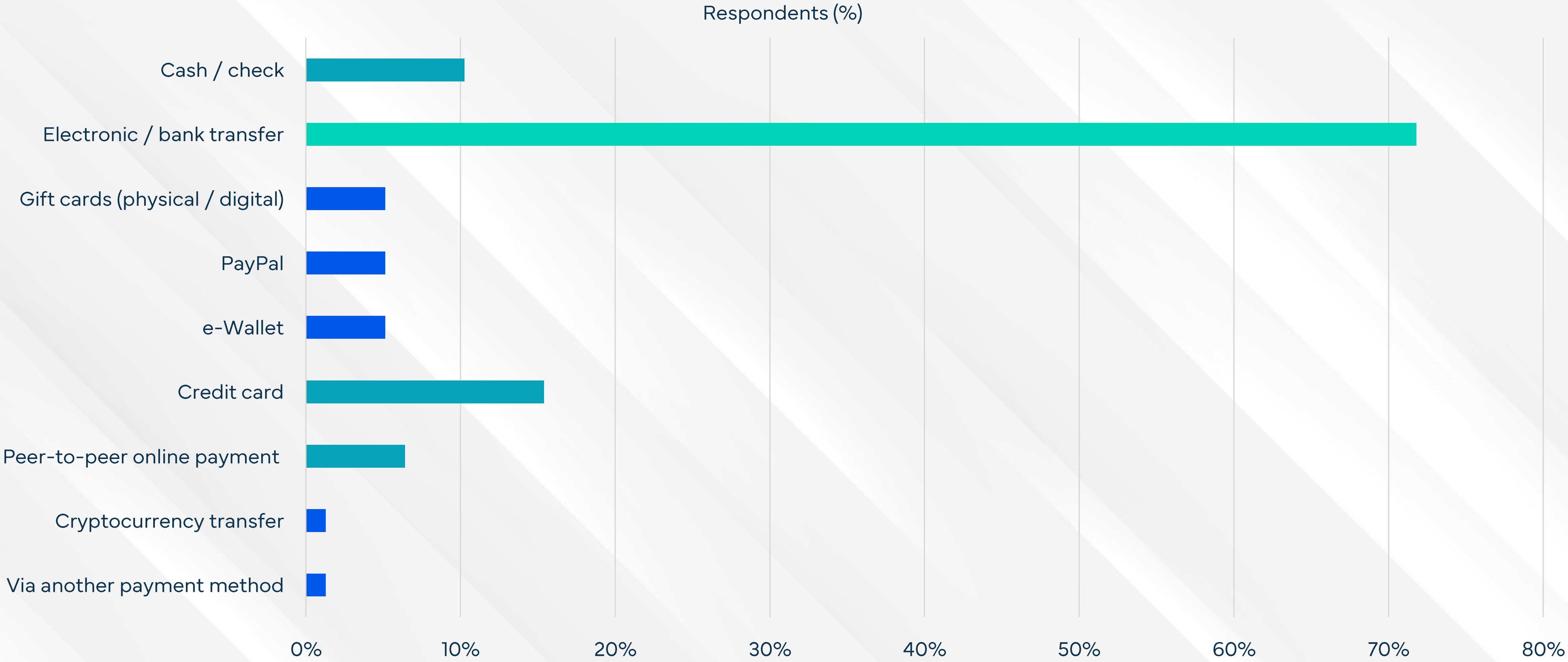
increase in South Korean scam losses, since 2023

In total, the South Korea lost US$12 billion to scams, which is equal to 0.7% of South Korea'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 account for 72% of scam payments in South Korea

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

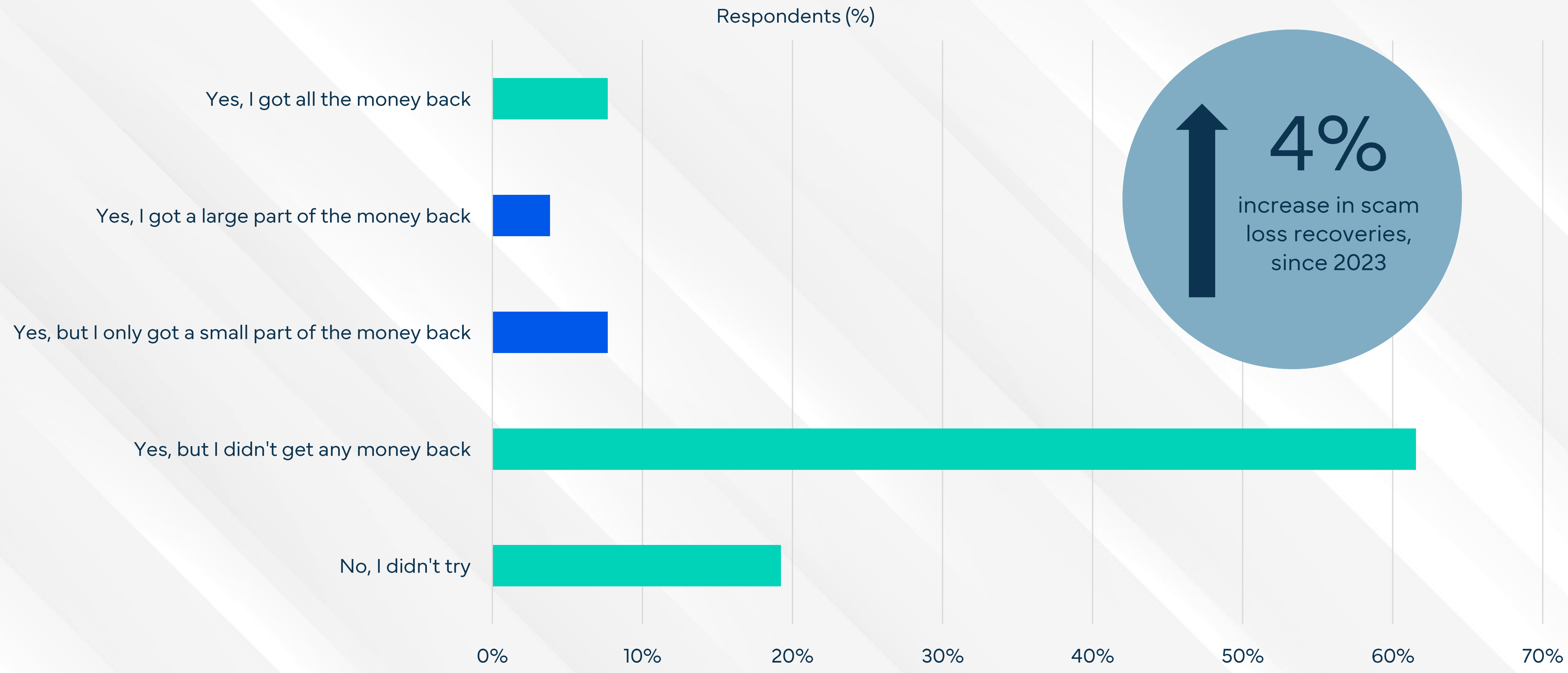


Credit cards, cash/checks & peer-to-peer payment methods also rank high on scam payment methods.

Q15 - How did you pay the scammer?

Only 8% of South Korean victims fully recovered their losses

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

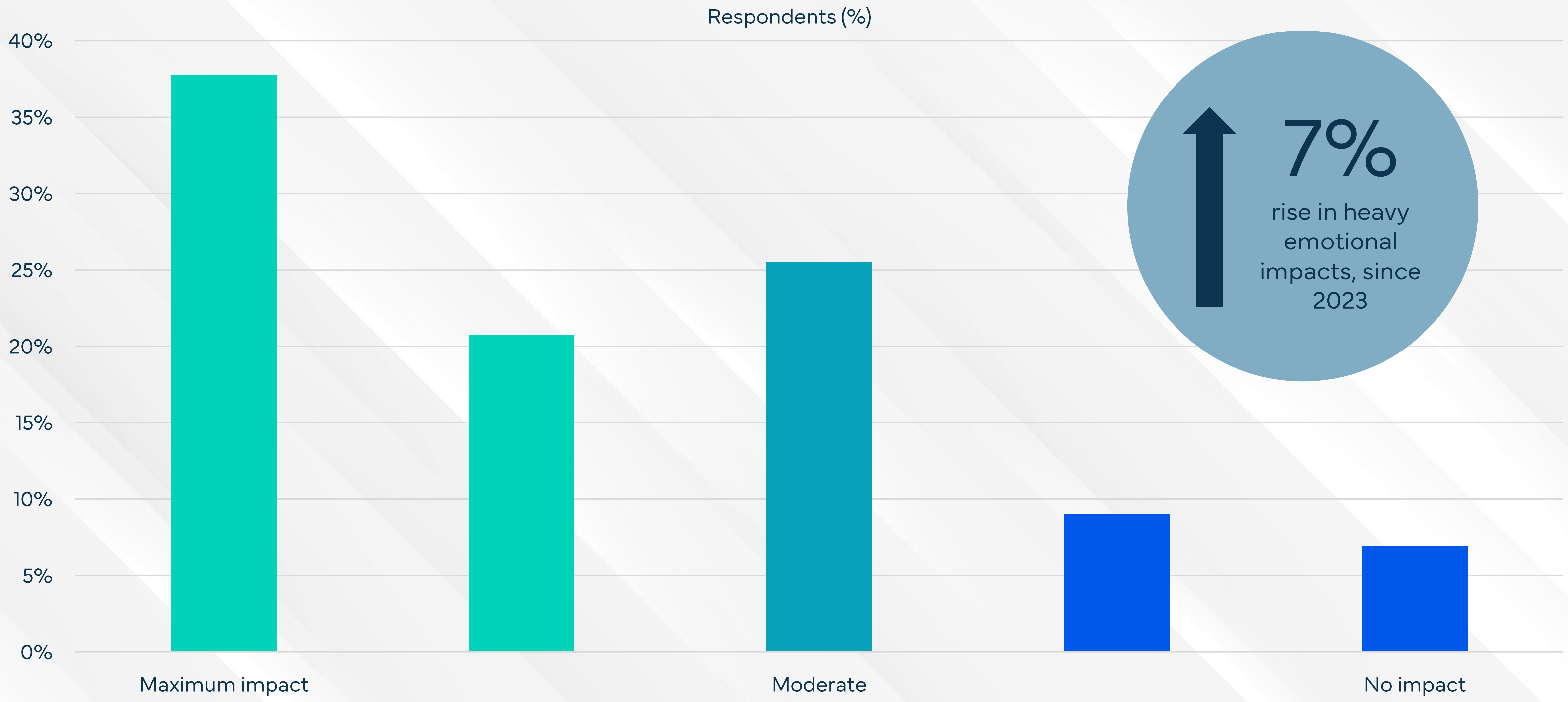


4% increase in scam loss recoveries, since 2023

19% did not try to recover their funds. 62% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

59% of South Korean scam victims perceive a strong emotional impact



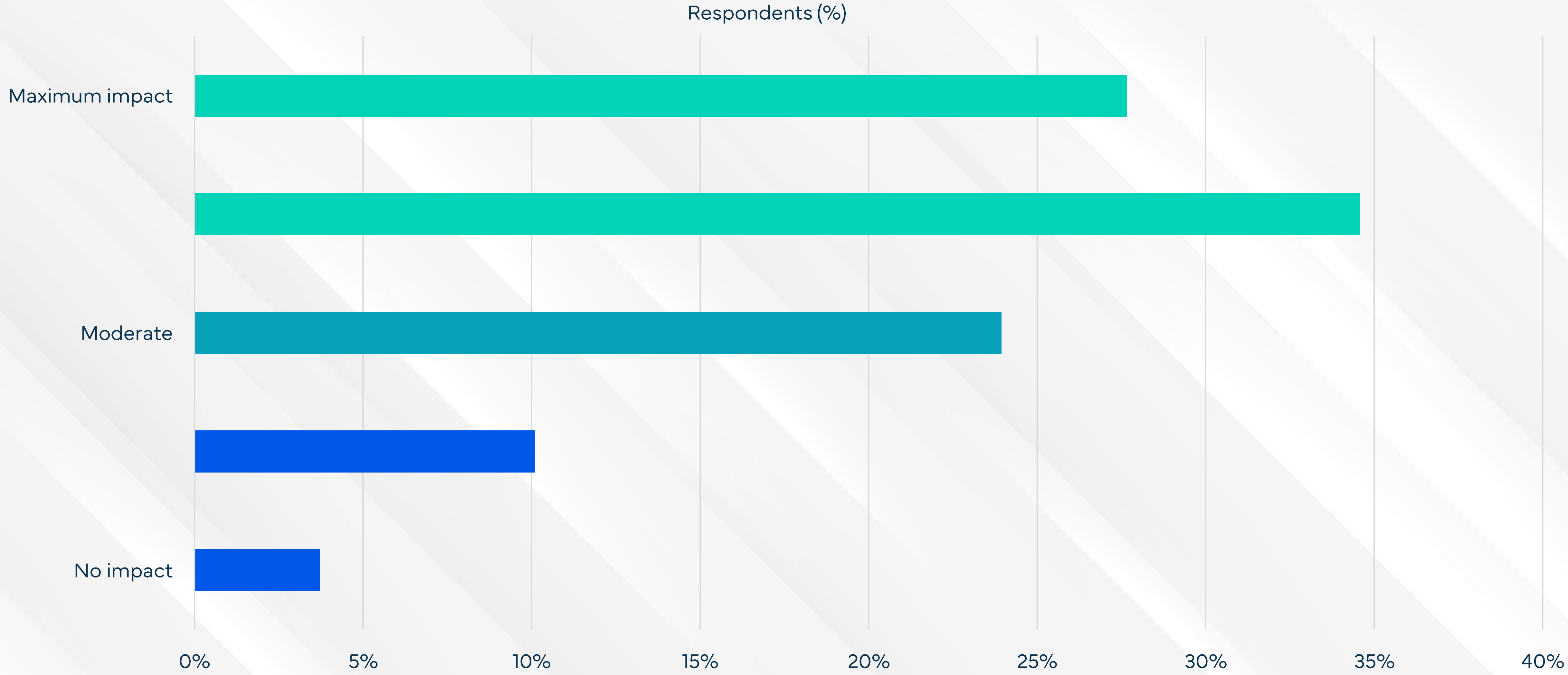
7%

rise in heavy emotional impacts, since 2023

16% of the survey respondents reported little to no emotional impact due to scams.

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

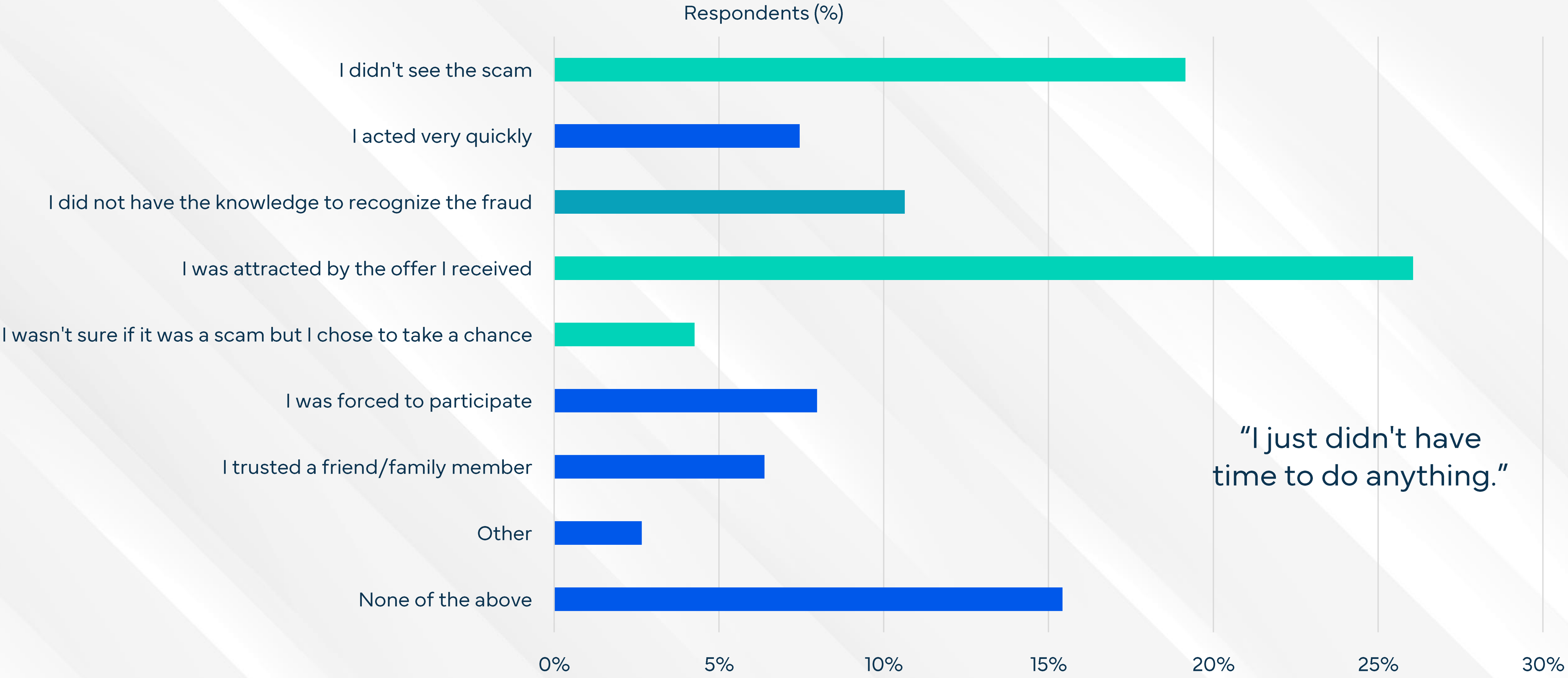
62% of South Korean have less trust in the Internet because of scams



Only 14% of South Korean 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?

South Koreans are often caught out by the offer made by scammers

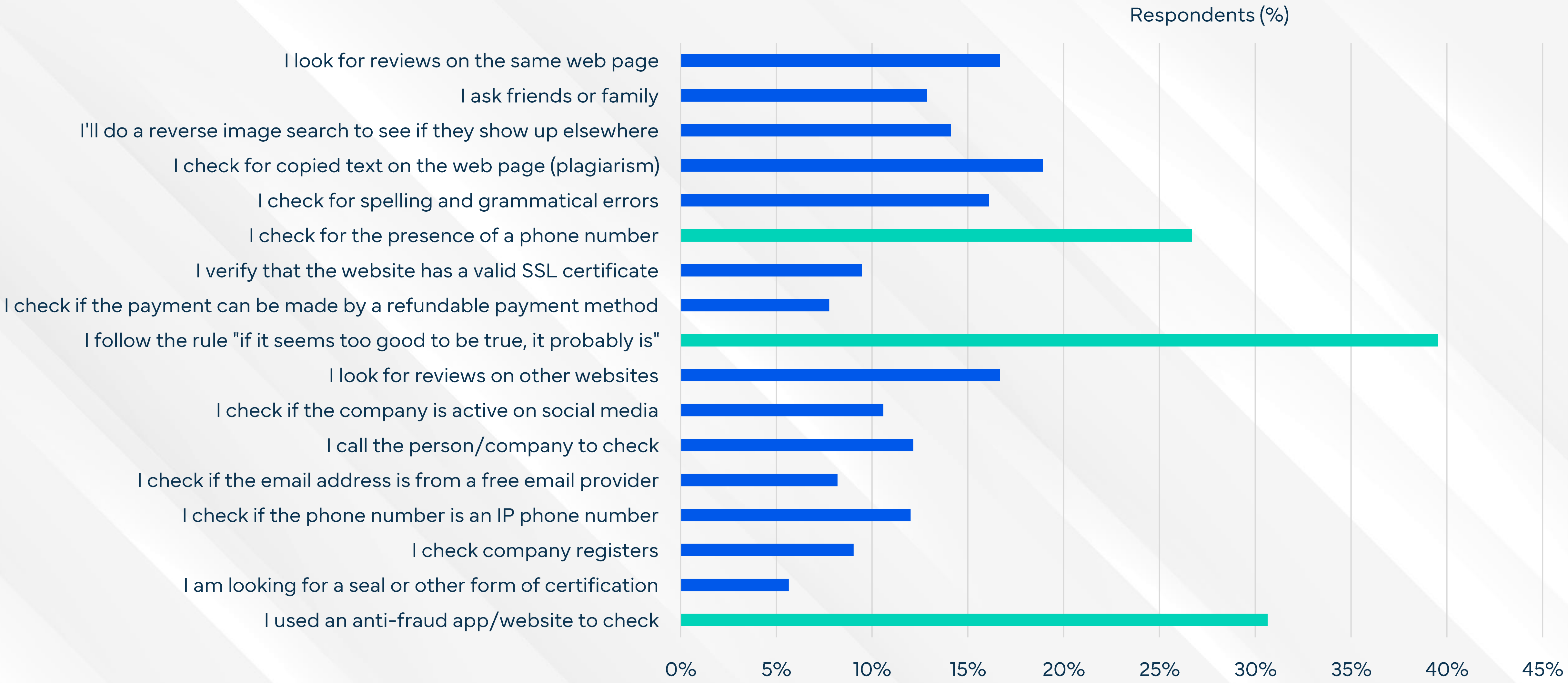


"I just didn't have time to do anything."

Several victims also reported inability to spot the scam while didn't have the knowledge to see the scam.

Q19 - What was the main reason you were deceived?

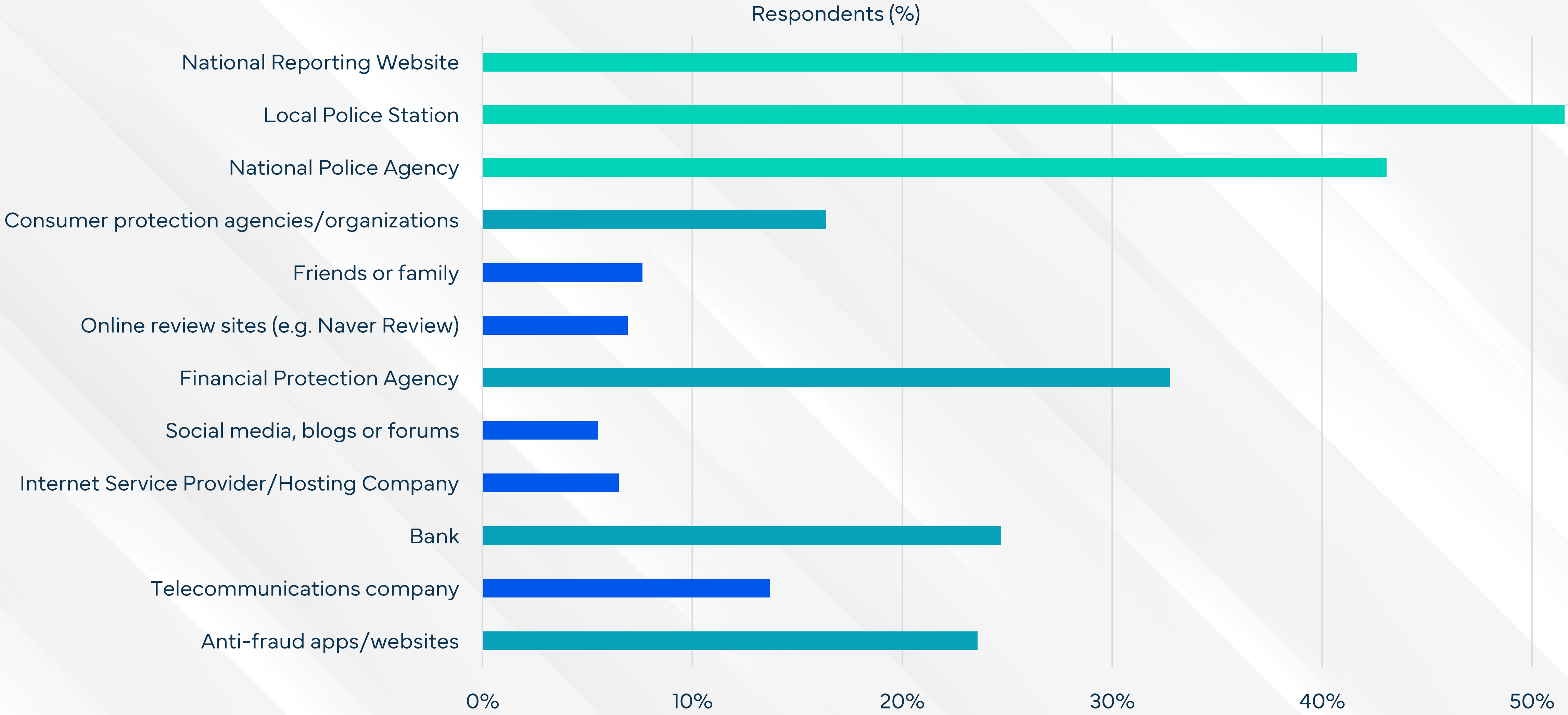
40% of the participants use "if it seems too good to be true" rule



Many reported using anti-fraud app/website and checking for the presence of a phone number.

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

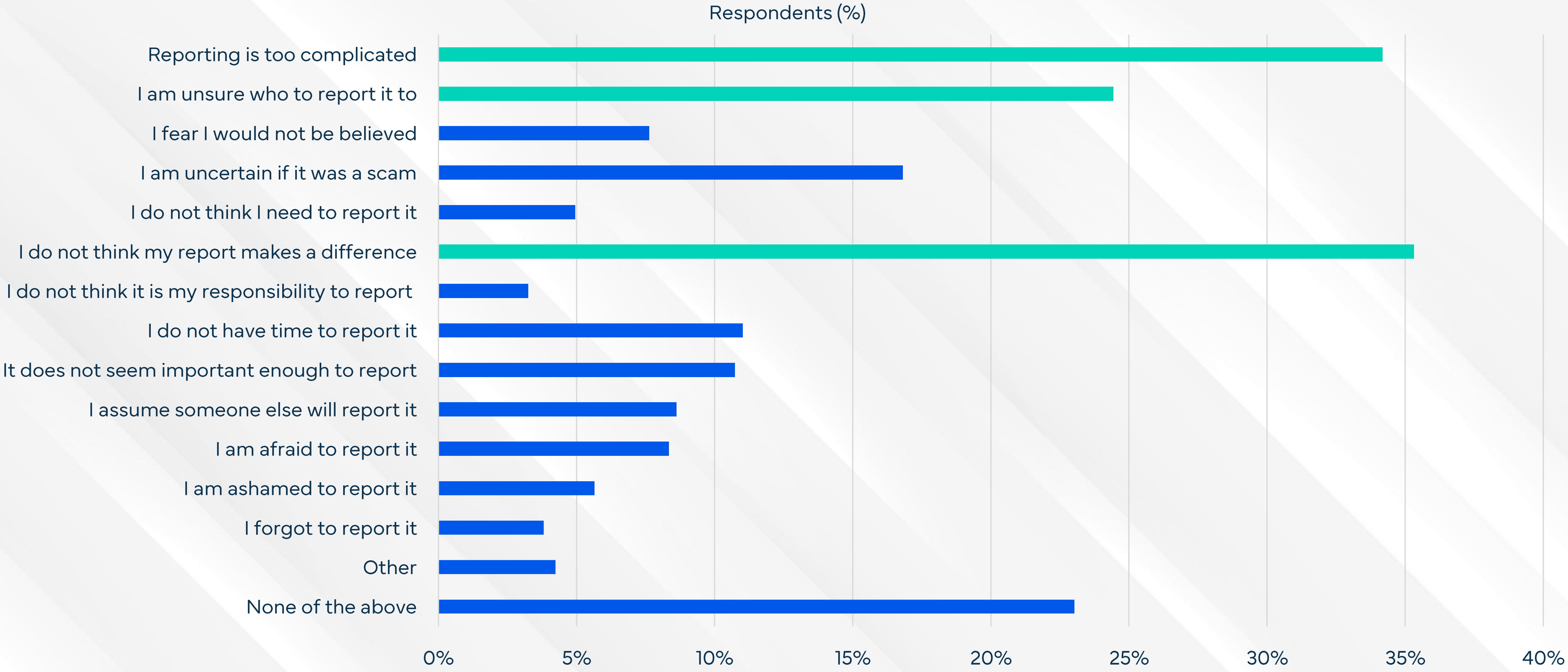
Scams are mostly reported to Police & National Reporting Website



Financial protection agency, Banks, & anti-fraud apps/sites are also popular places to report scams.

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

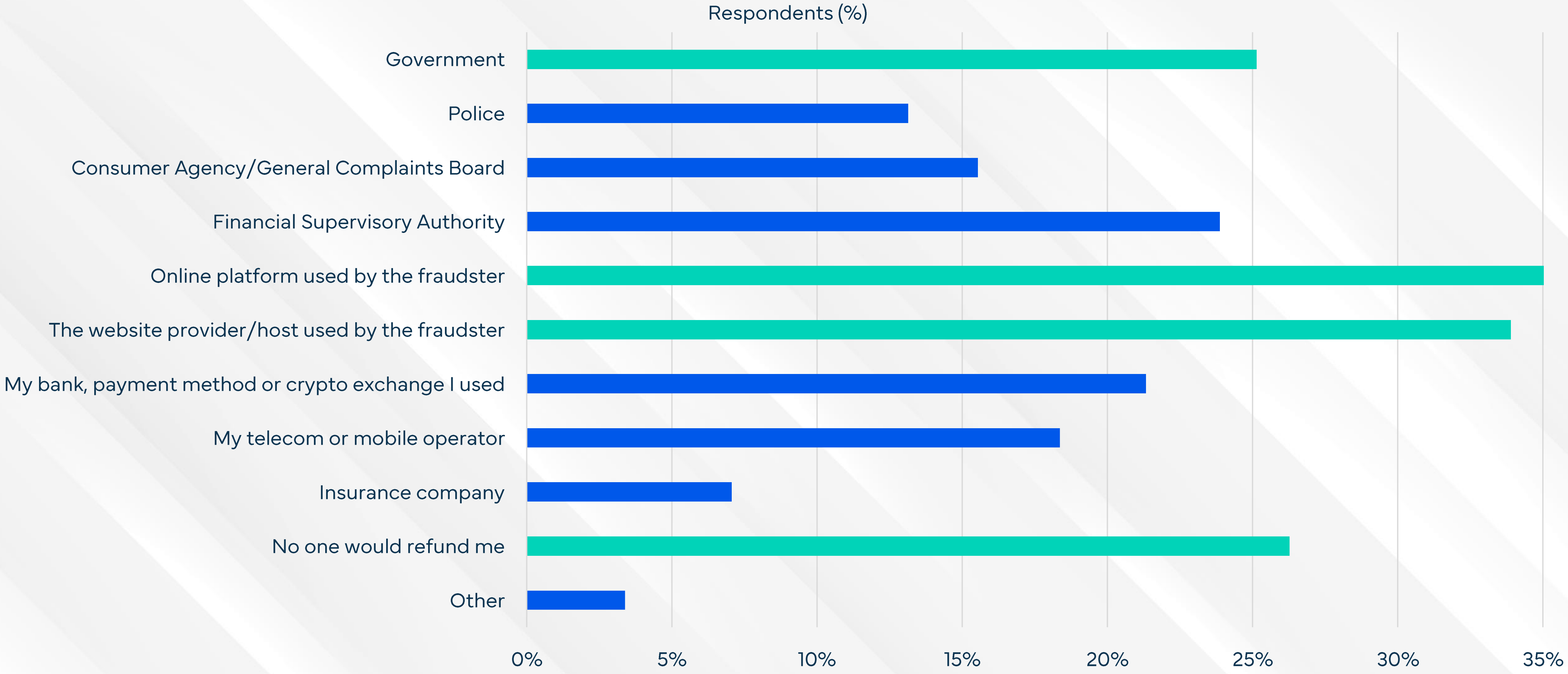
Reporting processes are seen as too complex and unlikely to fix anything



Another prominent reason for choosing not to report is an uncertainty of whom to report scams.

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

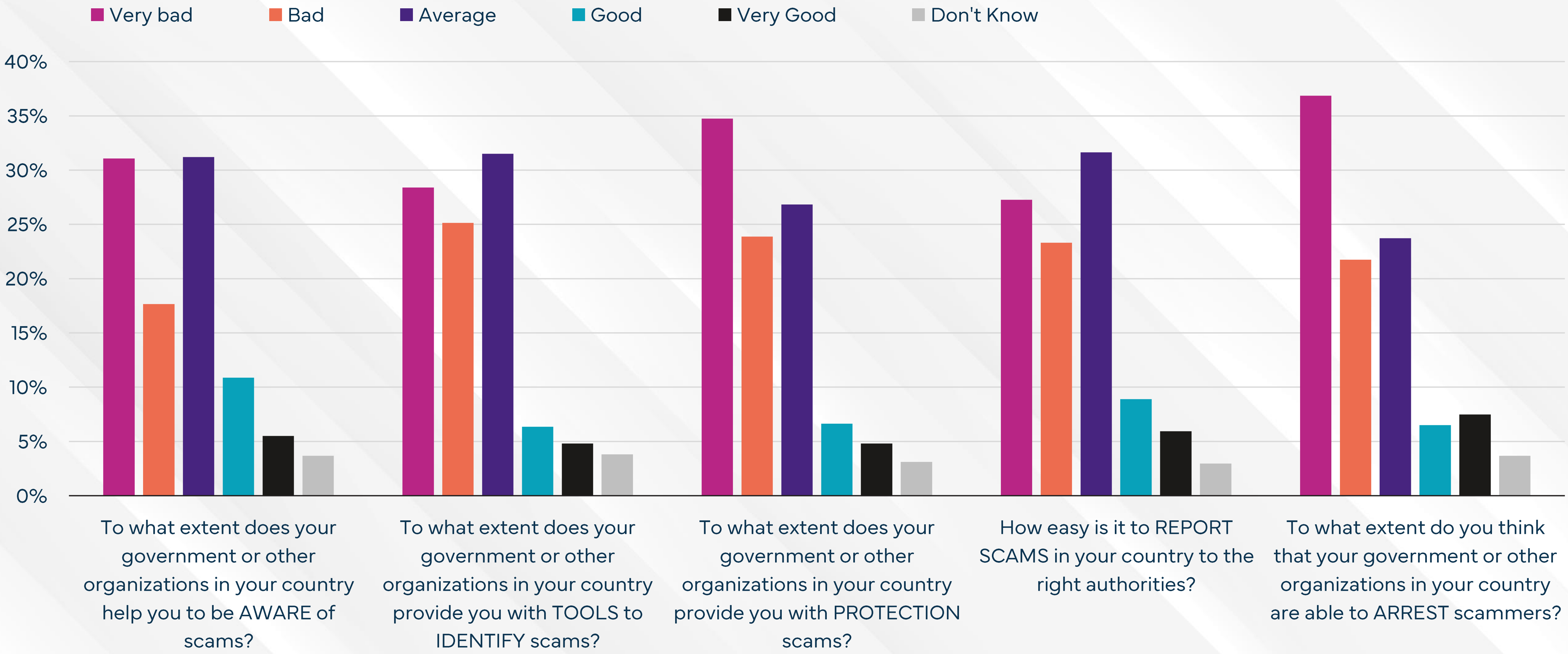
A quarter of the respondents assume no one will refund their scam losses



Others deem the online platform used, website host/provider, and government responsible.

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 the South Korea's attempts to arrest scammers



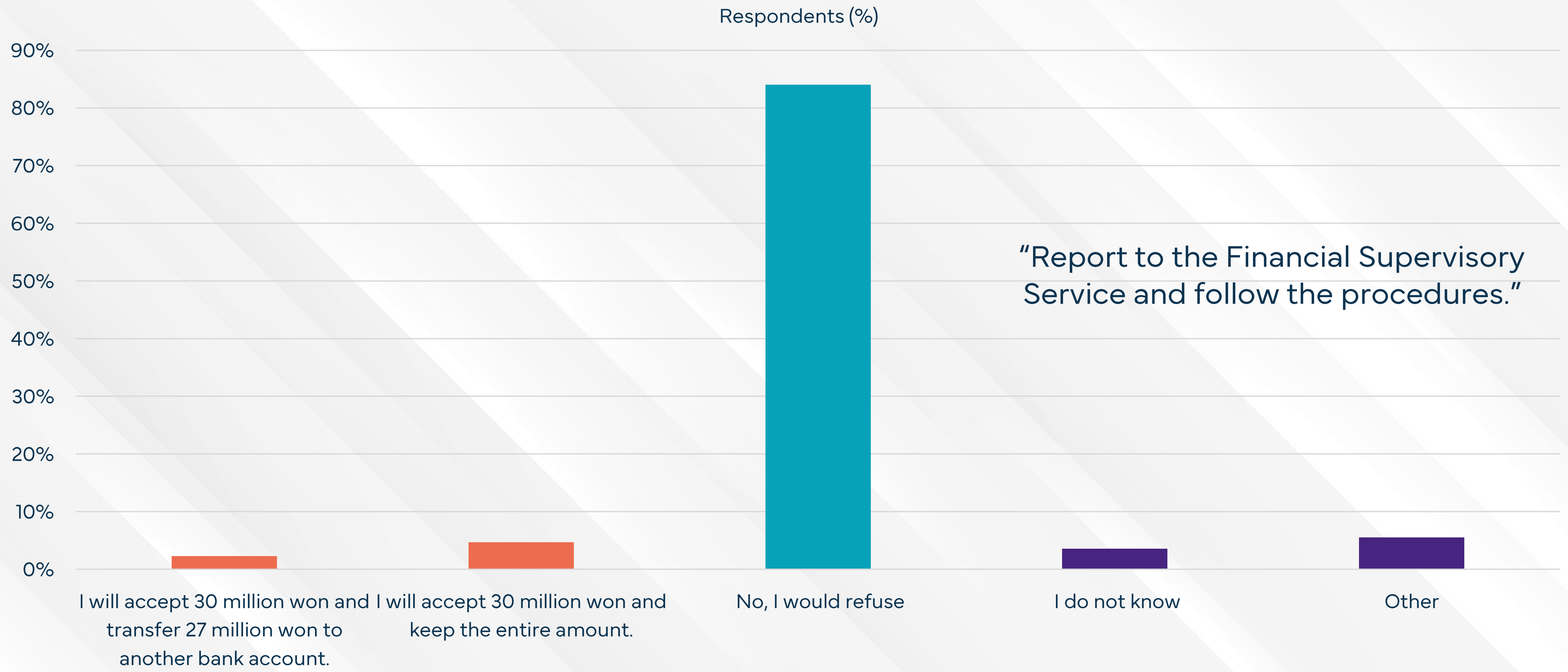
Overall, 54% of the participants rate the actions of the government as (very) bad, 14% as (very) good.

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?

2% of South Koreans admit that they would consider being a money mule

SCAMADVISER whoscall

GASA Global Anti-Scam Alliance



“Report to the Financial Supervisory Service and follow the procedures.”

However, 84% 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?

SCAMADVISER

whoscall

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.

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.

About the authors

SCAMADVISER whoscall GASA Global Anti-Scam Alliance

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

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
CapitalOne
feedzai
Gogolook
Google
SCAMADVISER
Meta
TREND MICRO
Match Group

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

SCAMADVISER
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

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