SCAMADVISER

whoscall

The State of Scams in Malaysia 2024

GASA

Global Anti-Scam Alliance

Fraudsters target 1-in-3 as Malaysians lose $12.8 billion in 12 months

The State of Scams in Malaysia 2024 report, conducted by the Global Anti-Scam Alliance (GASA) in partnership with Whoscall and Feedzai, provides a detailed analysis of scam trends affecting Malaysians. With data from 1,202 respondents, this study reveals both positive shifts and ongoing vulnerabilities in the nation's fight against scams.

While **52% of Malaysians feel confident in recognizing scams, up 2% from 2023, a significant 14% still lack confidence**. This persistent vulnerability suggests that while general awareness may be increasing, many Malaysians remain unsure of their ability to identify more sophisticated scams. This could be due to limited exposure to comprehensive anti-scam education, particularly on newer tactics involving AI-generated content.

Scams remain a pervasive issue, with **74% of Malaysians encountering scams monthly—a slight decrease from last year**. However, **43% reported an increase in scam encounters over the past year**, indicating that scammers are becoming more aggressive or finding new ways to exploit digital channels. **Phone calls, instant messaging apps, and social media** continue to be the primary methods for scam delivery, with a notable **8% increase in text and SMS scams since 2023**. Platforms like WhatsApp, Telegram, and Facebook remain heavily exploited, reflecting scammers' adaptation to popular communication tools.

Most Malaysians are aware that AI can be used in scams, particularly for generating chat and text. However, a quarter of respondents were unsure if AI was used in scams they encountered, showing a gap in understanding more advanced AI tools. This uncertainty could make Malaysians more susceptible to scams using newer technologies that are harder to detect.

Financial losses due to scams are substantial, with 32% of survey participants losing money to fraud. **The average loss per victim was $2,726, totalling $12.8 billion USD, or 3% of Malaysia's GDP**. This significant impact suggests that high-value scams, particularly investment frauds, are prevalent. The reliance on bank transfers and peer-to-peer payments for these scams indicates a focus on methods that are difficult to reverse, complicating recovery efforts.

Only 2% of victims managed to recover their losses, a sharp decline from last year's 8%. This decrease may be due to the increasing sophistication of scams, making it harder for victims to recover funds. Additionally, **70% of Malaysians did not report scams to law enforcement**, reflecting a 5% decline in reporting. This underreporting is likely due to scepticism about the effectiveness of reporting and the belief that it won't lead to a resolution. The complexity and perceived ineffectiveness of reporting processes contribute to this trend, indicating a need for accessible & transparent reporting systems.

Scams have a significant emotional toll, with **57% of victims experiencing a strong emotional impact**, up 2% from last year. This emotional strain, coupled with financial losses, has led to a decline in faith in digital platforms, with **63% of Malaysians reporting less trust in the Internet**. This eroded trust could have long-term consequences for digital engagement & economic activity.

Public dissatisfaction with government efforts to combat scams is high, with many Malaysians feeling that not enough is being done. The belief that reporting scams is ineffective, along with the perception of complex reporting processes, discourages many from seeking help. Additionally, the **open admission of 4% of Malaysians to consider becoming a money mule**, despite knowing the risks, indicates potential economic desperation and a lack of awareness about the consequences.

This report clearly signals a dire situation in Malaysia, with a huge chunk of the country's GDP disappearing into the pockets of fraudulent actors. While there has been some progress in scam awareness, almost all hope has been lost for victims in recovering the stolen funds. We cannot reiterate enough, that for the battle to protect Malaysians from scams to succeed, the government urgently needs to introduce enhanced public education, better reporting mechanisms, and stronger law enforcement action.

Jorij Abraham
Managing Director

GASA
Global Anti-Scam Alliance

Sam Rogers
Director of Marketing

Malaysia needs to enhance scam education and detection capabilities

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 Malaysia and the advanced strategies needed for enterprises to protect consumers.

How significant has the issue of scams become in Malaysia?

The State of Scams in Malaysia 2024 report reveals that 74% of Malaysians encounter scams at least once per month, and 43% reported an increase in scam attempts. Cases related to phishing, fraud and scam have risen tremendously, and caused financial losses of $12.8 billion last year, amounting to 3% of Malaysia's GDP. This amount of losses is not the absolute figure as the report says 70% of victims did not report the scam to authorities.

What types of scams have trended in Malaysia recently?

Investment scams are showing an upward trend based on statistics. This finding is consistent with the statistics from PDRM Bukit Aman Commercial Crime Investigation Department (CCID), where a total of 8,655 investment scams had been recorded since last year resulting in RM875.4mil in losses. Statement from PDRM said among the modus operandi used by the syndicate was to promote purported syariah compliant-investment products, where scammers will also claim that their investments are certified by the Securities Commission or Bank Negara Malaysia in order to dupe victims.

Telegram is one of the most common communication mediums exploited in investment scams, followed by Facebook and WhatsApp. These mediums are commonly used for online scams, especially love scams. With increasingly sophisticated tactics, electronic bank transfers and peer-to-peer payments dominate scam transactions. Victims often suffer significant emotional and psychological damage, with only 13% reporting little to no emotional impact, highlighting the severe trust issues these scams create.

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 Malaysian government has taken proactive steps to combat scams by establishing the National Scam Response Center 997 (NSRC 997) and launching a dedicated reporting channel for scam-related incidents. Public awareness campaigns are being conducted by various parties such as PDRM, finance institutions, telecommunications companies, to keep reminding people alert about trending scams.

Cybersecurity Malaysia has strengthened its commitment through MOUs with the leading TrustTech company, while the Royal Malaysia Police (PDRM) continues its efforts with the #ScamFreeMalaysia initiative. Pos Malaysia Berhad has also partnered with the TrustTech company to implement anti-scam measures, including certified numbers and a nationwide awareness campaign.

These joint efforts between the government and businesses educate the market, equipping Malaysians with knowledge on scam prevention, helps them protect themselves and their families from potential scams.

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

Despite increased government attention to the issue of scams, Malaysians are currently hesitant to report incidents, often due to difficulty recognizing scams. This underscores the need for enhanced scam-related education and effective detection tools to verify malicious attempts. Collaboration between businesses and the government is crucial to developing a comprehensive protection shield against the growing scam problem. By working together, we can strengthen defenses and create a safer digital environment for everyone.

Aaron Chiou
Product Director
SCAMADVISER

Public-private collaboration is the key to kicking scams out of Malaysia

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 **2024 State of Scams in Malaysia report**, GASA interviewed **Manwoo Joo, COO of Gogolook** to share insights on the in-depth analysis of the evolving scam landscape in Malaysia, 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 Malaysia?

The scale of scams in Malaysia has reached a critical level, with losses amounting to $12.8 billion last year, representing 3% of the nation's GDP. This highlights the widespread nature of the issue, affecting individuals across various demographics.

However, it is deeply concerning that 70% of victims do not report these incidents to the relevant authorities, leaving scammers unchecked. We need to foster a reporting culture and adopt best practices from other markets where digital literacy and transparency play a key role in reducing scam vulnerabilities.

What types of scams have trended in Malaysia recently?

Over the past year, we've seen a surge in AI-powered scams, which are becoming increasingly sophisticated and harder for consumers to identify, adding to the challenge.

The recent statistics from Bukit Aman Commercial Crime Investigation Department indicated that love scams are still on the rise, where more than two-thirds of love scam victims are women, and losses almost RM24mil from January to August this year.

Social media platform Telegram has been flagged by the police as the platform of choice for online scammers. Among 16 social media applications found to be most commonly used by scammers, Telegram topped the list, followed by Facebook and WhatsApp.

As for investment scams, the police had recorded 3,863 cases from January to August this year, with losses estimated to be around RM484mil.

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 government and organizations are actively working to combat these threats through public awareness campaigns, stronger regulatory measures, and partnerships with financial institutions to enhance fraud detection systems.

Authorities such as Royal Malaysia Police's (PDRM) commercial crimes investigation department (CCID) has regularly shared the latest trends of scam activities in Malaysia, at the same time working closely & innovatively with strategic partners like Whoscall in fighting online crimes and protecting the public. Public are advised to check suspicious bank account numbers, phone numbers or company names on the PDRM Semak Mule app or https://semakmule.rmp.gov.my/ and to contact the NSRC at 997 if they suspect they have fallen prey to any scam.

PDRM, Whoscall and Pos Malaysia have teamed up under Whoscall's national #ScamFreeMalaysia initiative to strengthen efforts against phone scams and parcel scams in Malaysia. With the scam number data shared by PDRM, and operation numbers shared by Pos Malaysia, Whoscall users can trust incoming calls and SMS, safeguarding Malaysians against the increasing threat of scams.

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

Moving forward, I would urge a collective effort in strengthening consumer education, especially in understanding the evolving nature of scams, including those driven by AI. More collaborative efforts between the private sector, authorities, and consumers will give the public the tools and confidence they need to stay one step ahead of scammers.

Lastly, anti-scam tools like Whoscall could be the first guard against various types of scam attempts. Be smart & stay alert all the time would be the best practice for prevention.

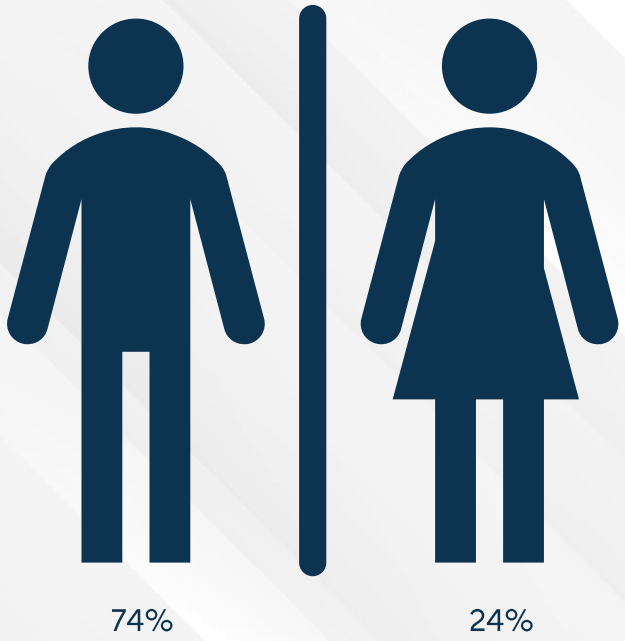
Manwoo Joo
COO
Gogolook
(Developer of Whoscall)

1,202 Malaysians completed the State of Scams survey

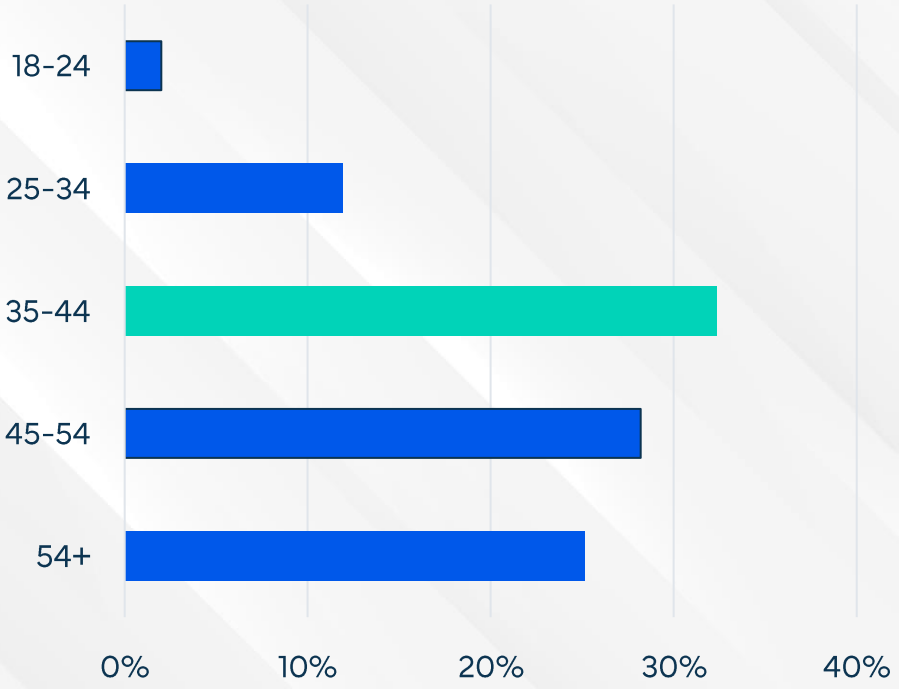
SCAMADVISER whoscall

GASA Global Anti-Scam Alliance

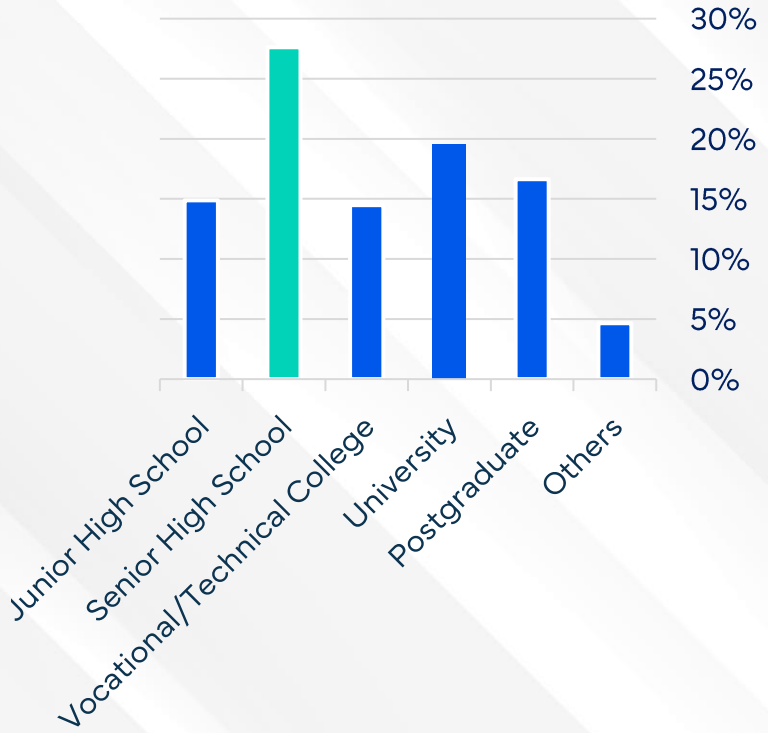
Gender



Age Range



Education



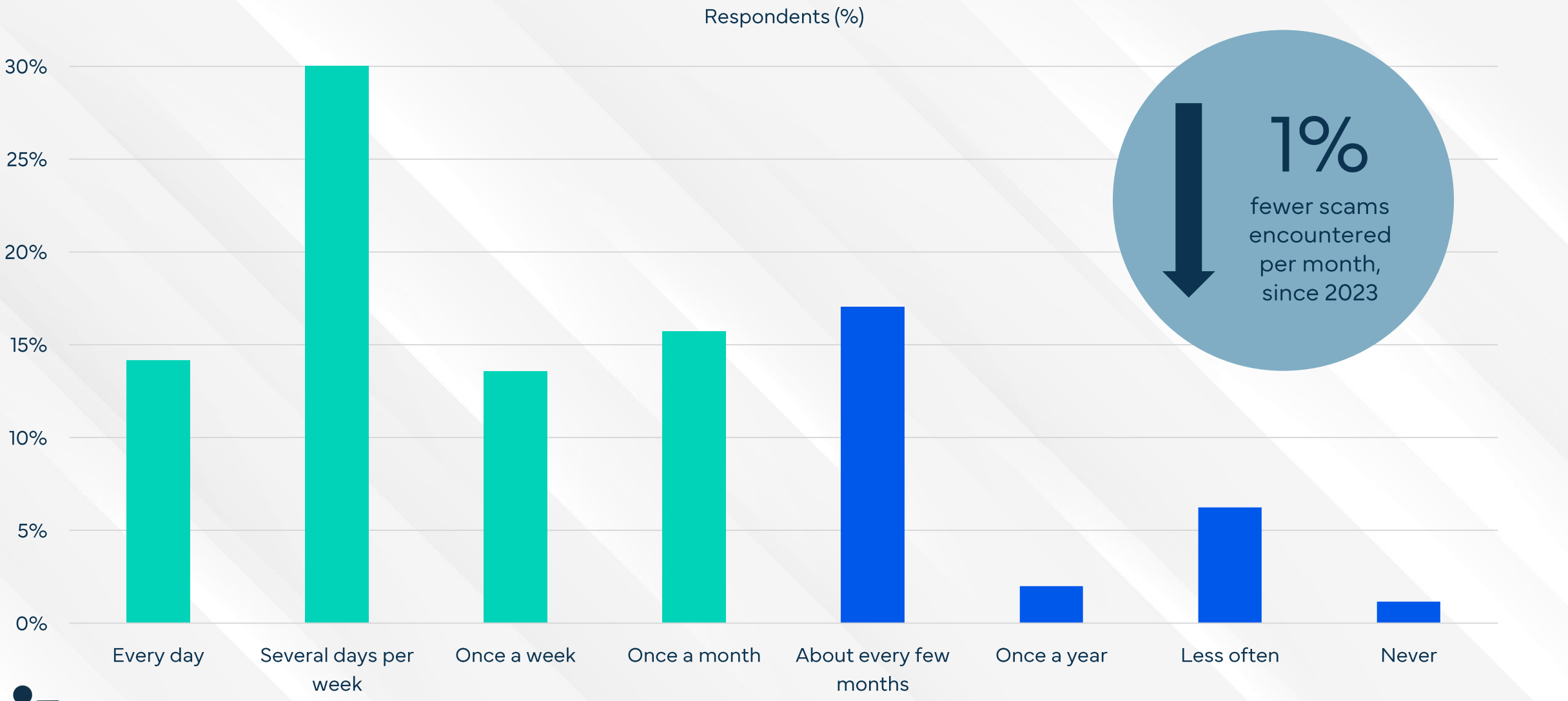
The demography of respondents to the State of Scams in the Malaysia 2024 survey consists of more men than women. A large proportion were aged 35-44, with senior high school education.

52% of Malaysians are confident in their ability to recognize scams

Only 14% of respondents are not (very) confident in recognizing scams, at all.

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

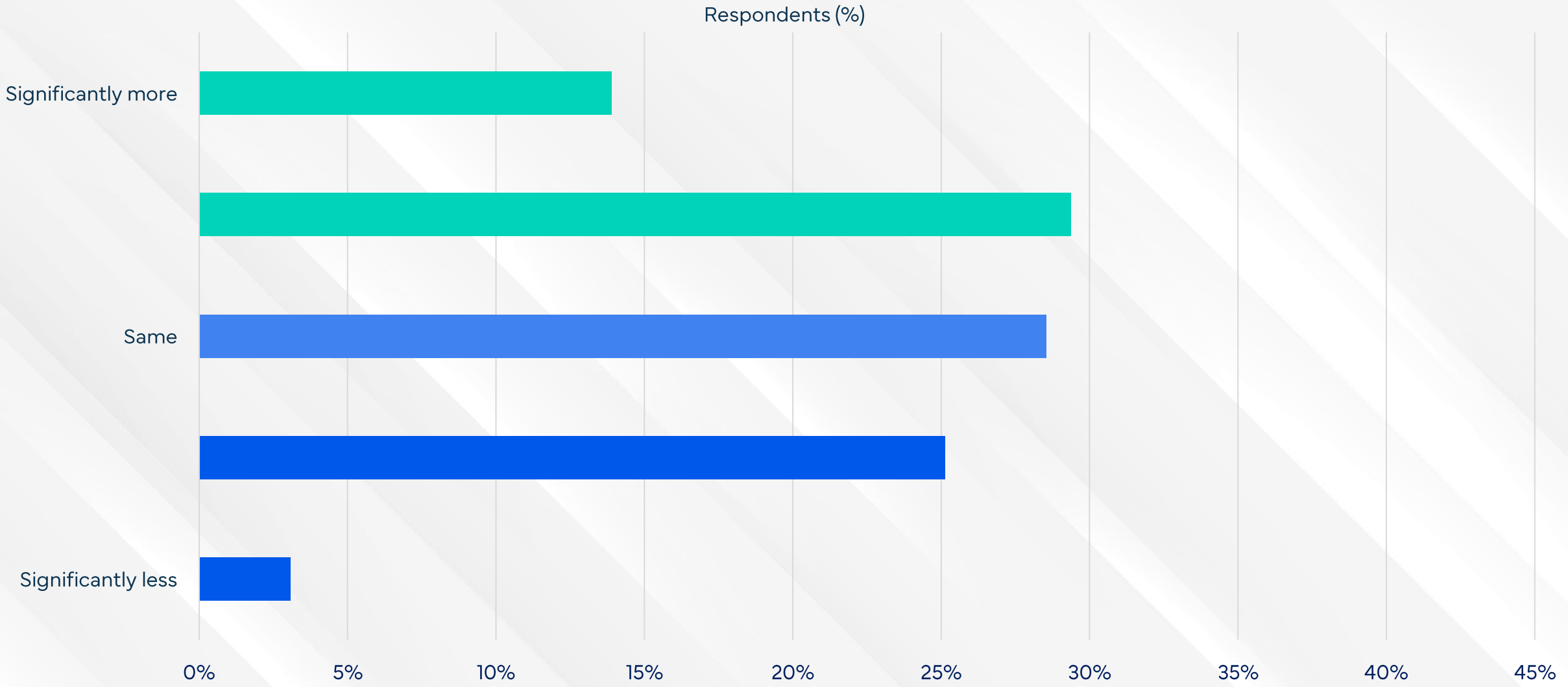
74% of Malaysians encounter scams at least once per month



8% of Malaysian respondents encountered fewer scams this year, compared to the previous 12 months.

Q3 - In the last 12 months, how often have you been exposed to scam attempts? This includes receiving suspicious content, as well as seeing deceitful advertising.

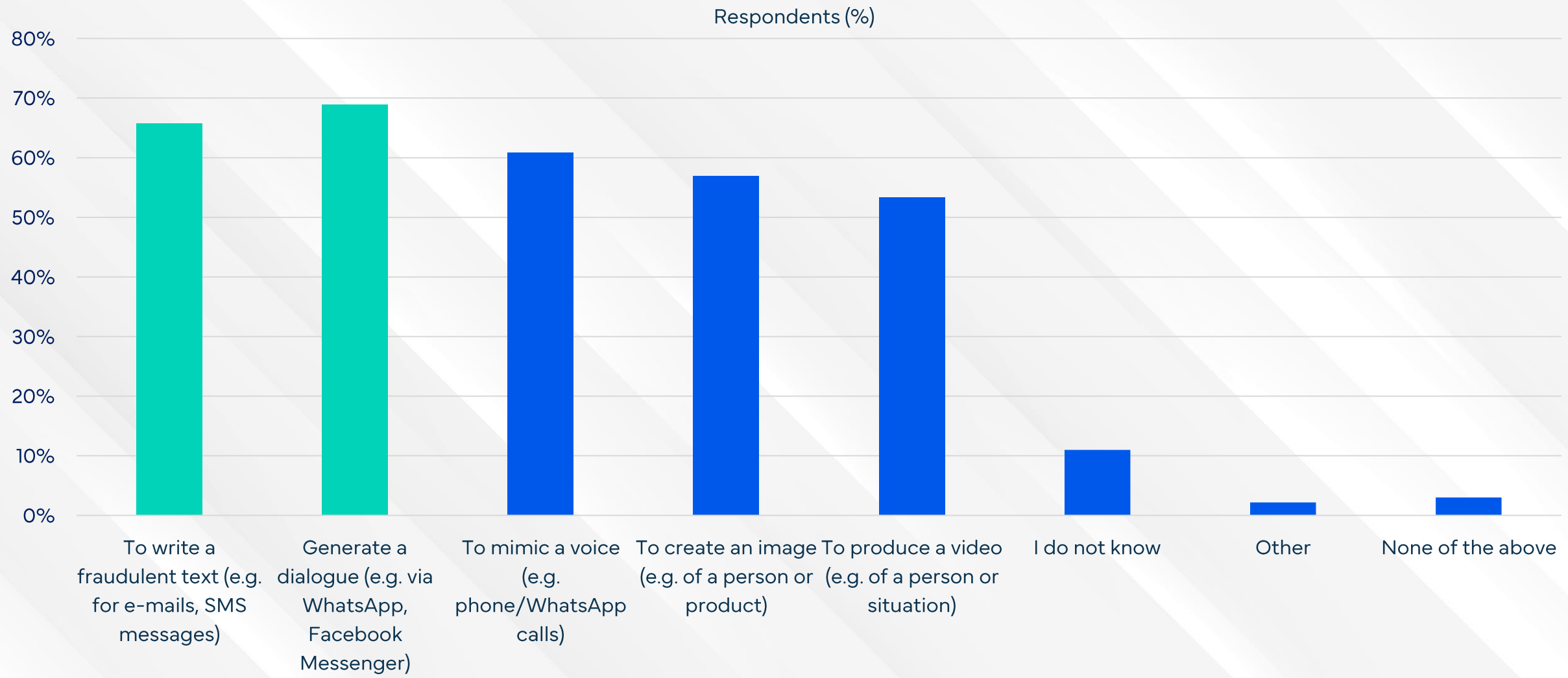
43% of Malaysians faced more scam encounters in the last 12 months



Only 28% of Malaysian 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?

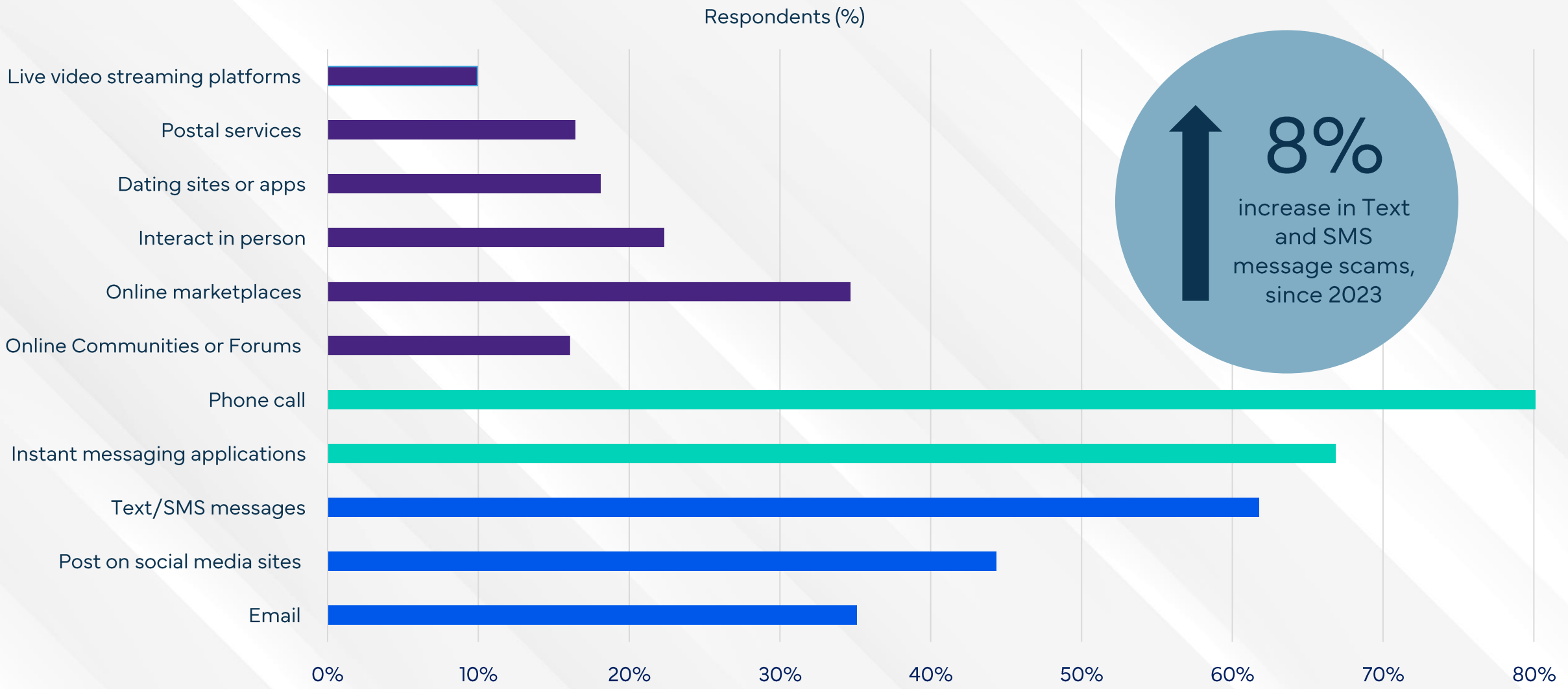
Most Malaysians are aware scammers can use AI against them



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

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

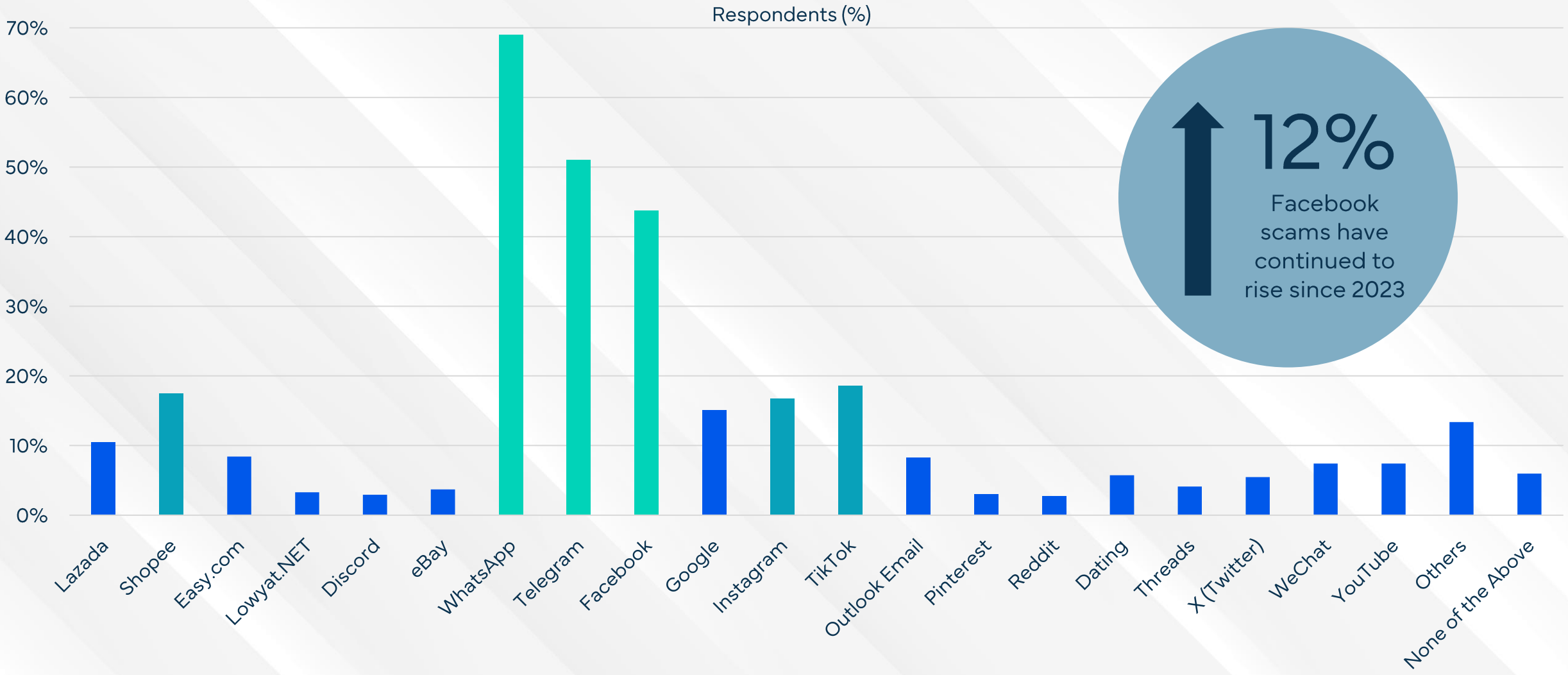
Majority of scams are delivered via Phone calls or instant messaging apps



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

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

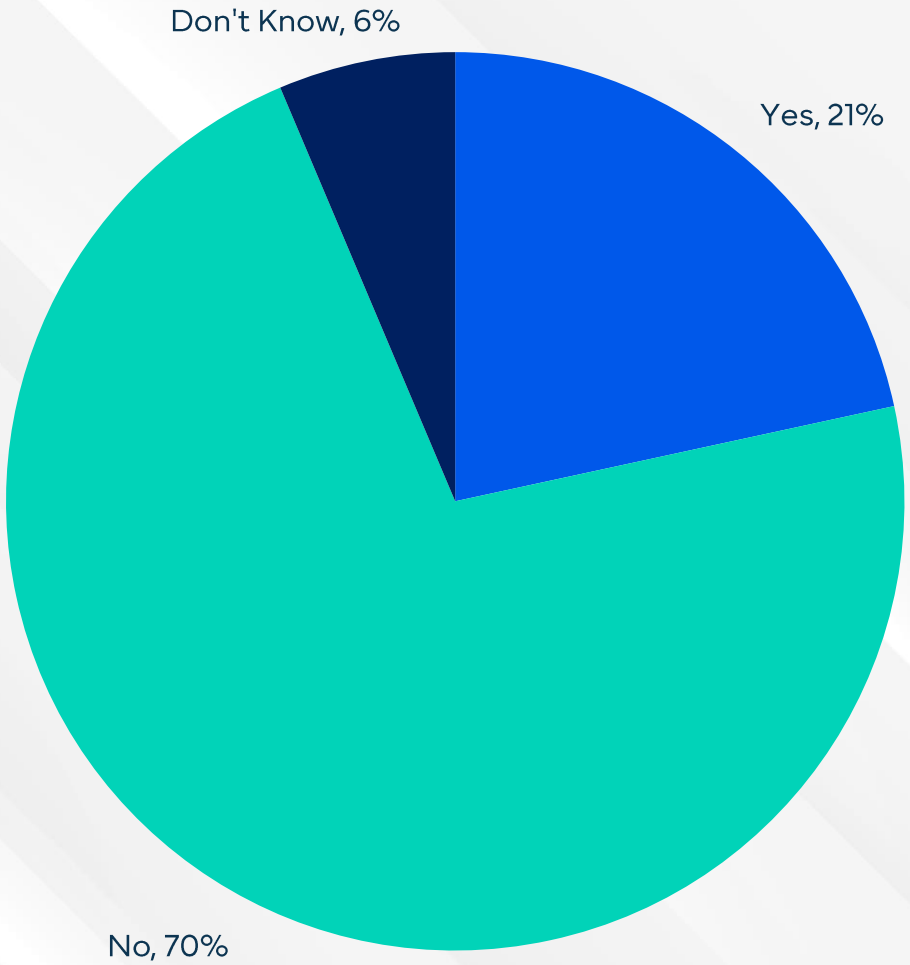
WhatsApp, Telegram, & Facebook are the most exploited platforms



TikTok and Shopee round out the top five platforms where people encounter scams.

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

70% of Malaysians did not report the scam to law enforcement

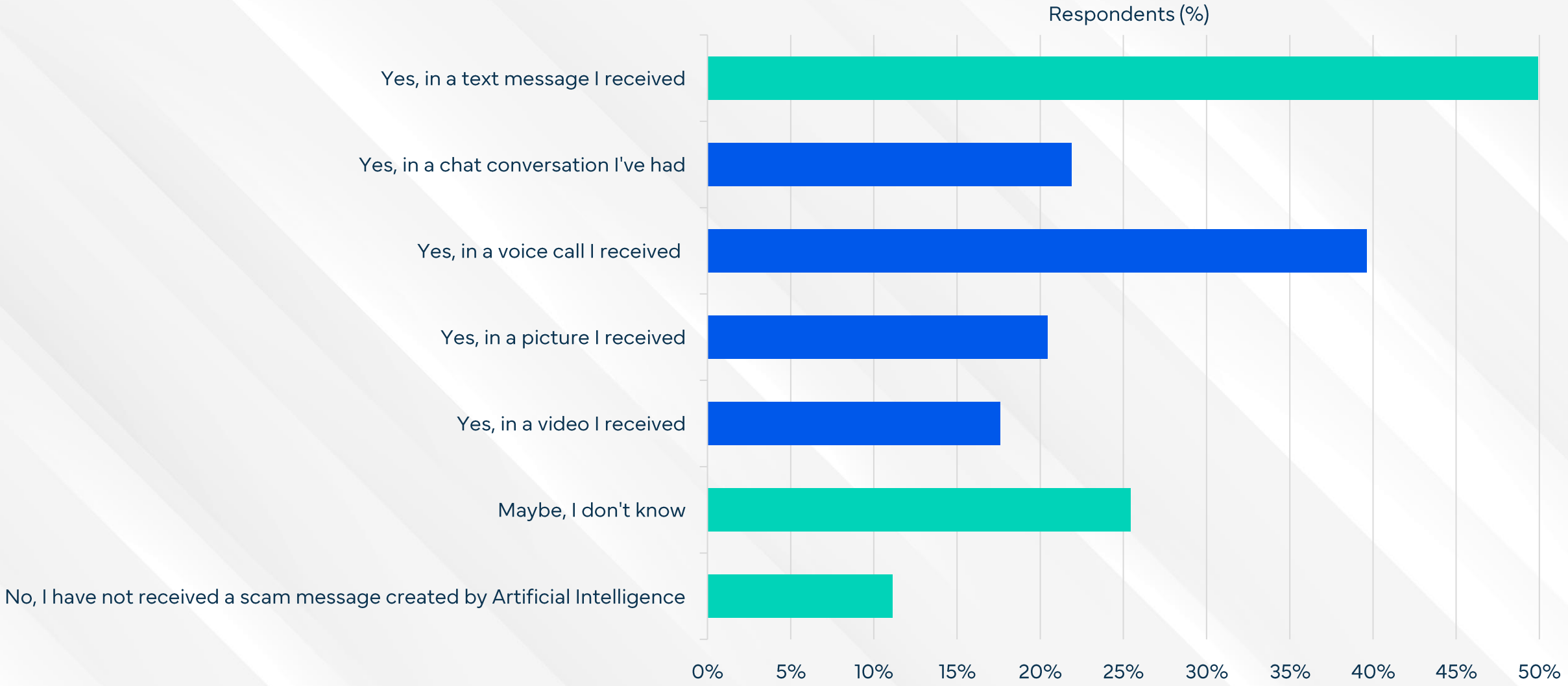


5%
fewer Malaysians report scams to law enforcement

21% 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?

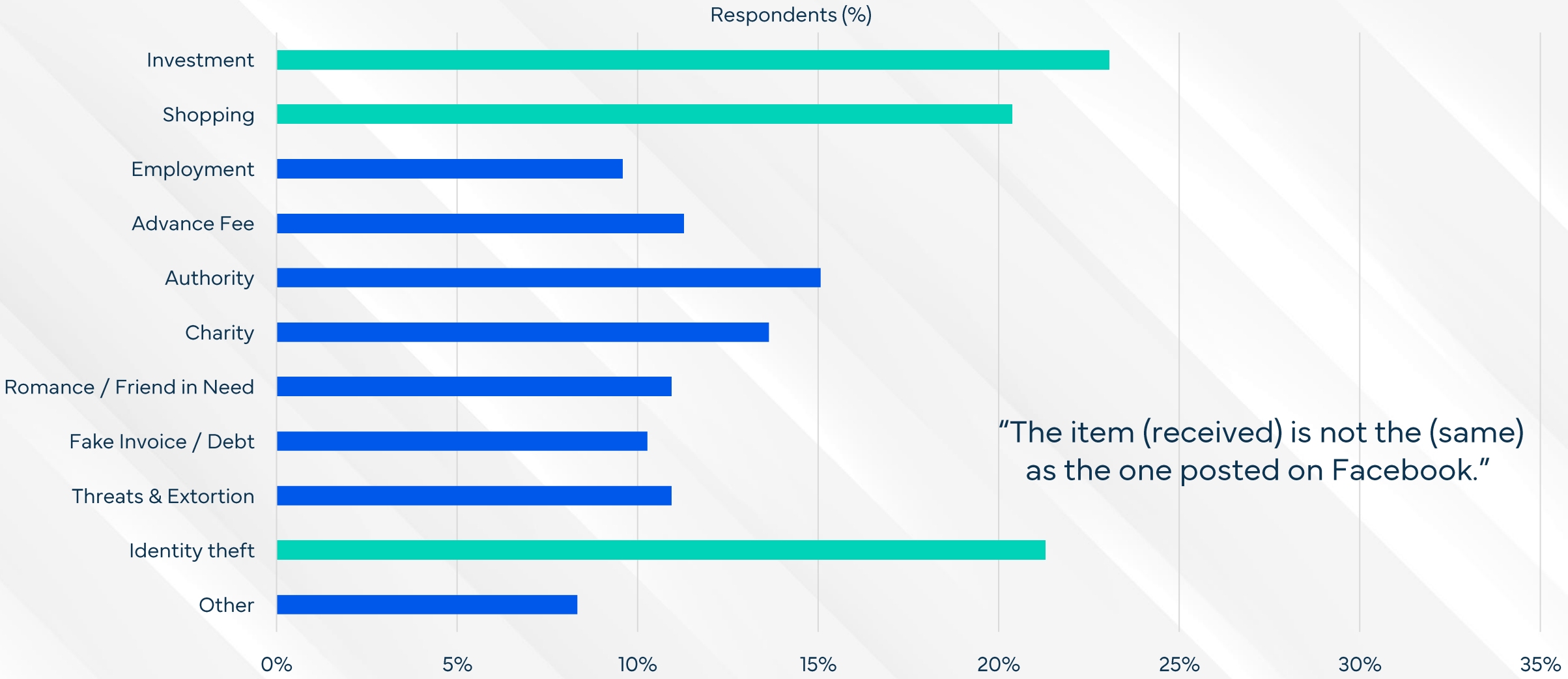
25% of Malaysians were uncertain whether AI was used to scam them



11% of Malaysians 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?

Investment Scams are the most common type of scam in Malaysia



"The item (received) is not the (same) as the one posted on Facebook."

41% did not fall victim to the most common scams in the last year. 1.55 scams were reported per victim.

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

Malaysian scam victims share their stories

SCAMADVISER whoscall

GASA Global Anti-Scam Alliance

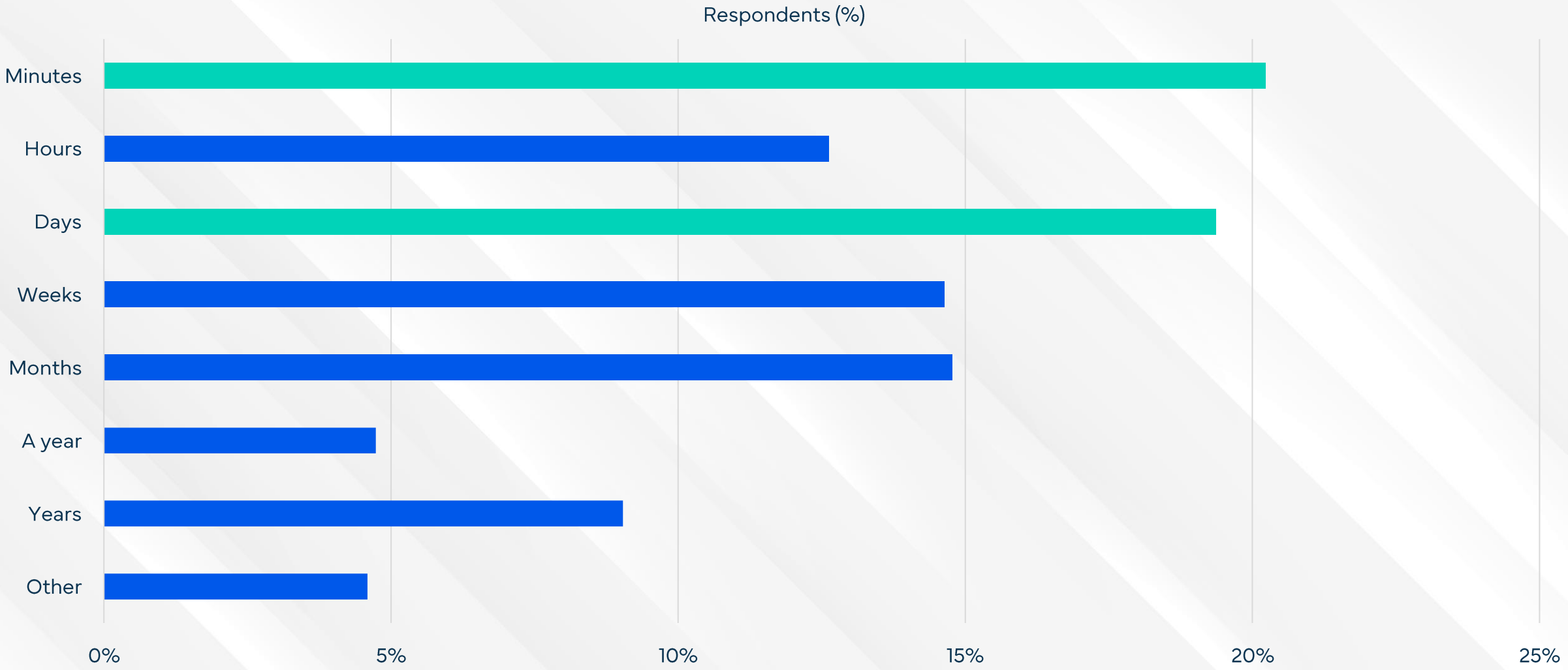
"Scams offering house cleaning services via Telegram. I was asked to make a deposit payment via QR touch & go of RM100. After the payment was made, I was immediately blocked from contacting the account."

"The scammer has threatened to spread false sexual information to family members if payment is not made. Payment of RM600 has been made 5 times."

"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."

"My credit card is used for online purchases abroad. I only realized it even received a bank statement. I made a report to the bank and got my money back."

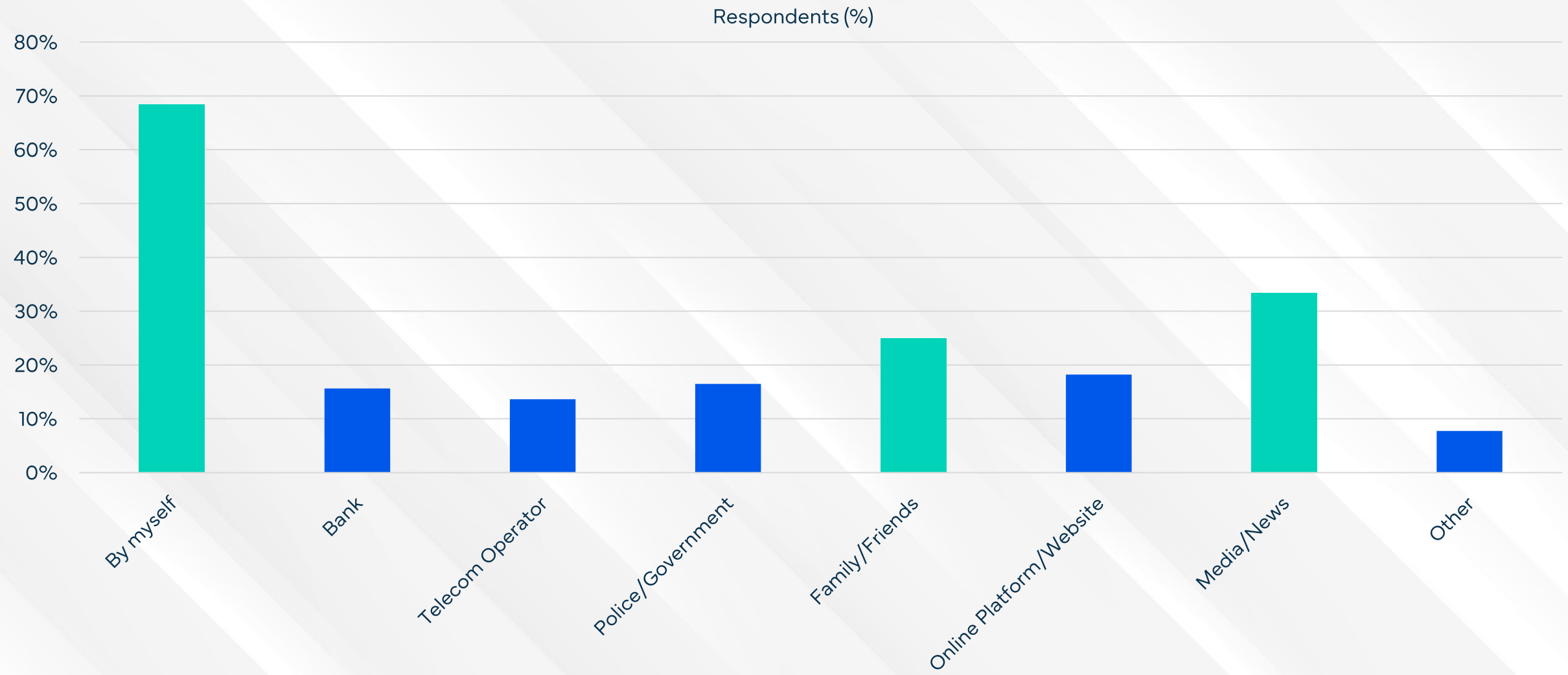
33% of scams are completed within 24 hours of first contact



20% reported scams that were over in minutes, while 14% 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?

68% of the victims realized on their own they had been scammed

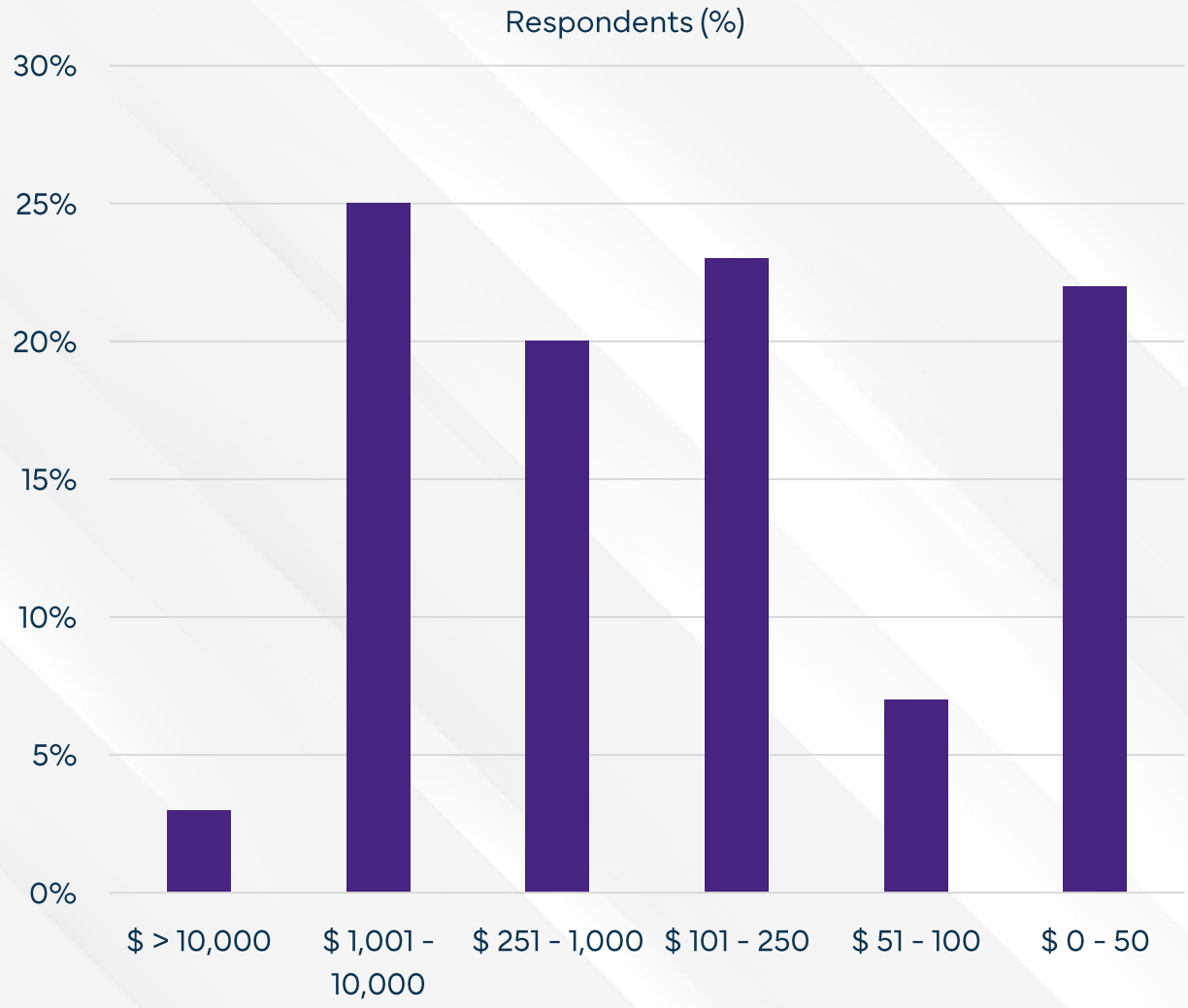


Others were informed by media/news, while family/friends are also popular in pointing out scams.

Q13 How did you discover you were scammed?

In total, 32% of Malaysian participants lost money in a scam

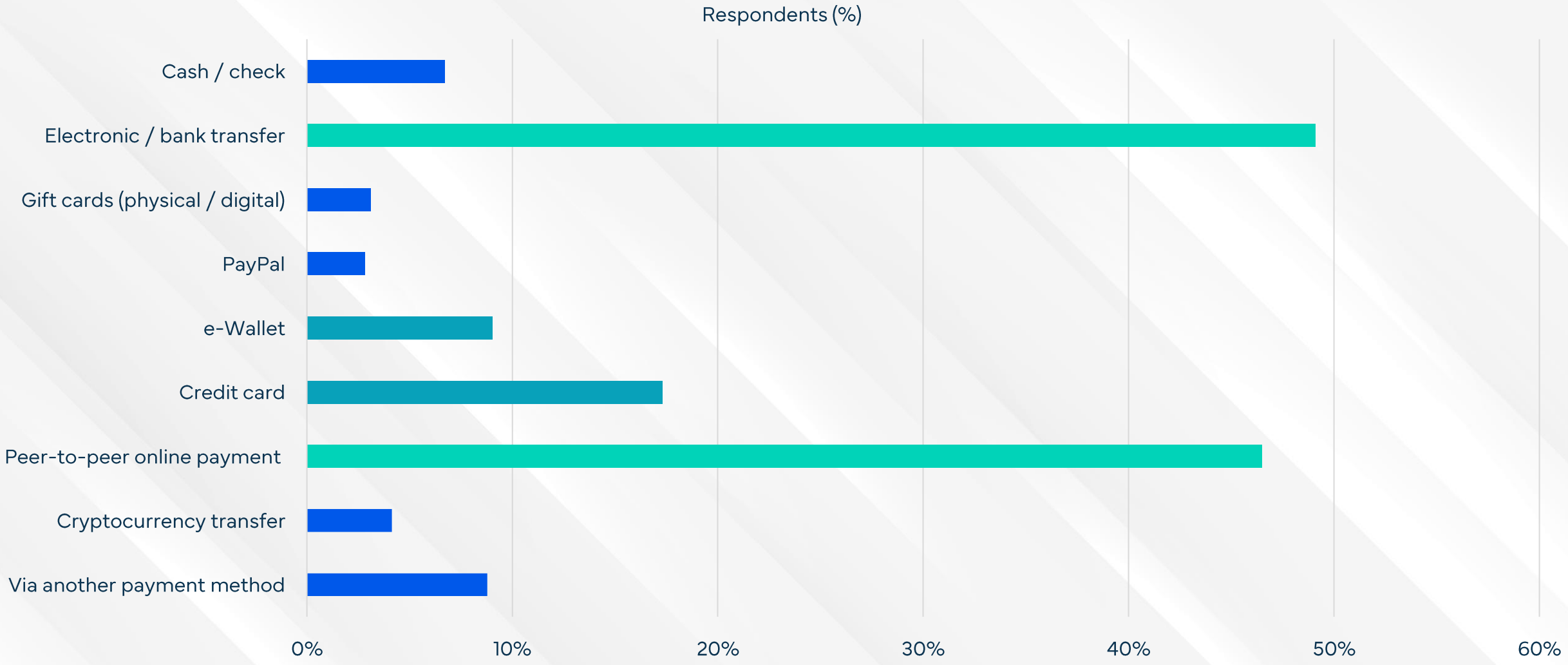
Survey Key Statistics	
Persons approached	1,202
Participants completing the survey	100%
Participants losing money	387
% losing money / approached persons	32%
Average amount lost in US Dollars	2,726
Total country population	34,564,810
Population over 18 years	25,351,089
# of people scammed > 18 years	8,162,123
Total scam losses (USD)	12,814,532,584
Total scam losses (MYR)	56,674,150,155
Gross Domestic Product (USD, millions)	430,895
% of GDP lost in scams	3%



In total, the Malaysians lost $12.8 billion to scams, which is equal to 3% of Malaysia's GDP.

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

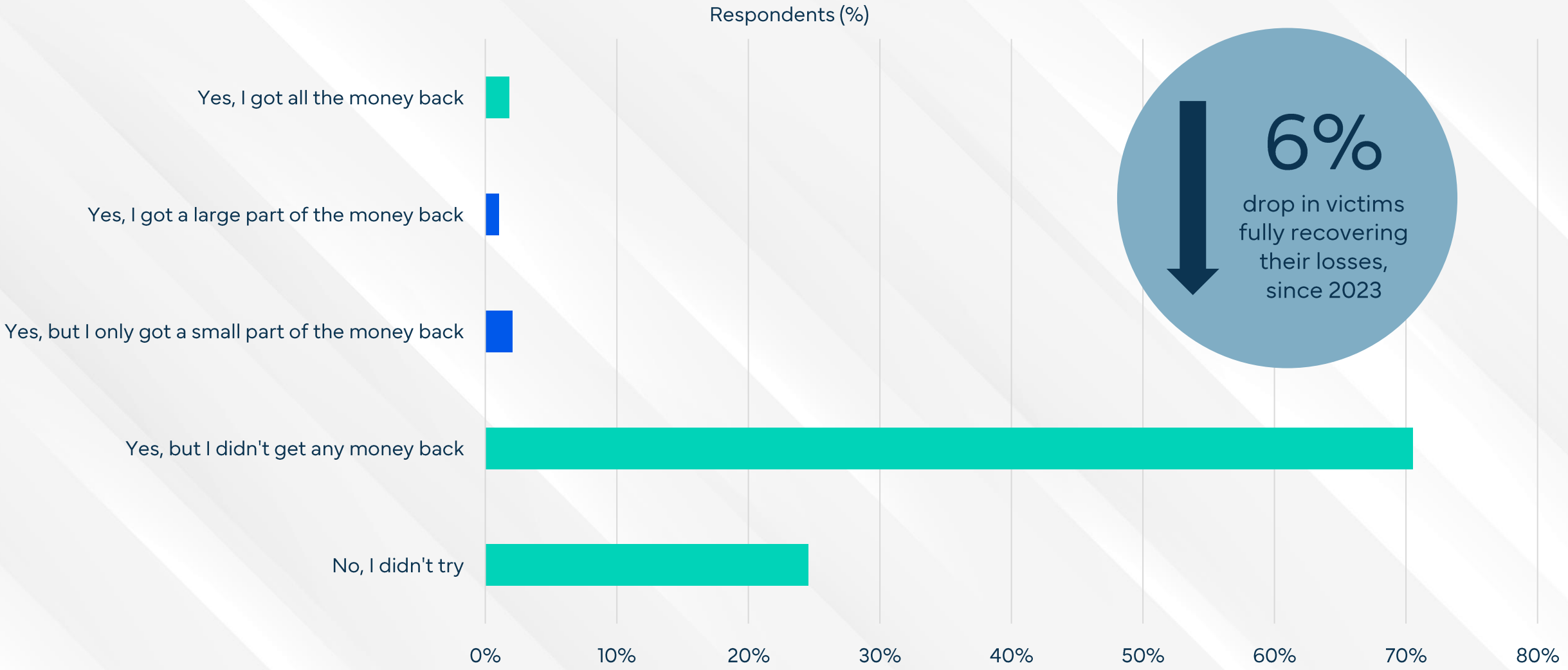
Bank Transfers & peer-to-peer payment dominate scam payments



Credit cards and e-wallets are also popular methods for scammers to collect their stolen gains.

Q15 - How did you pay the scammer?

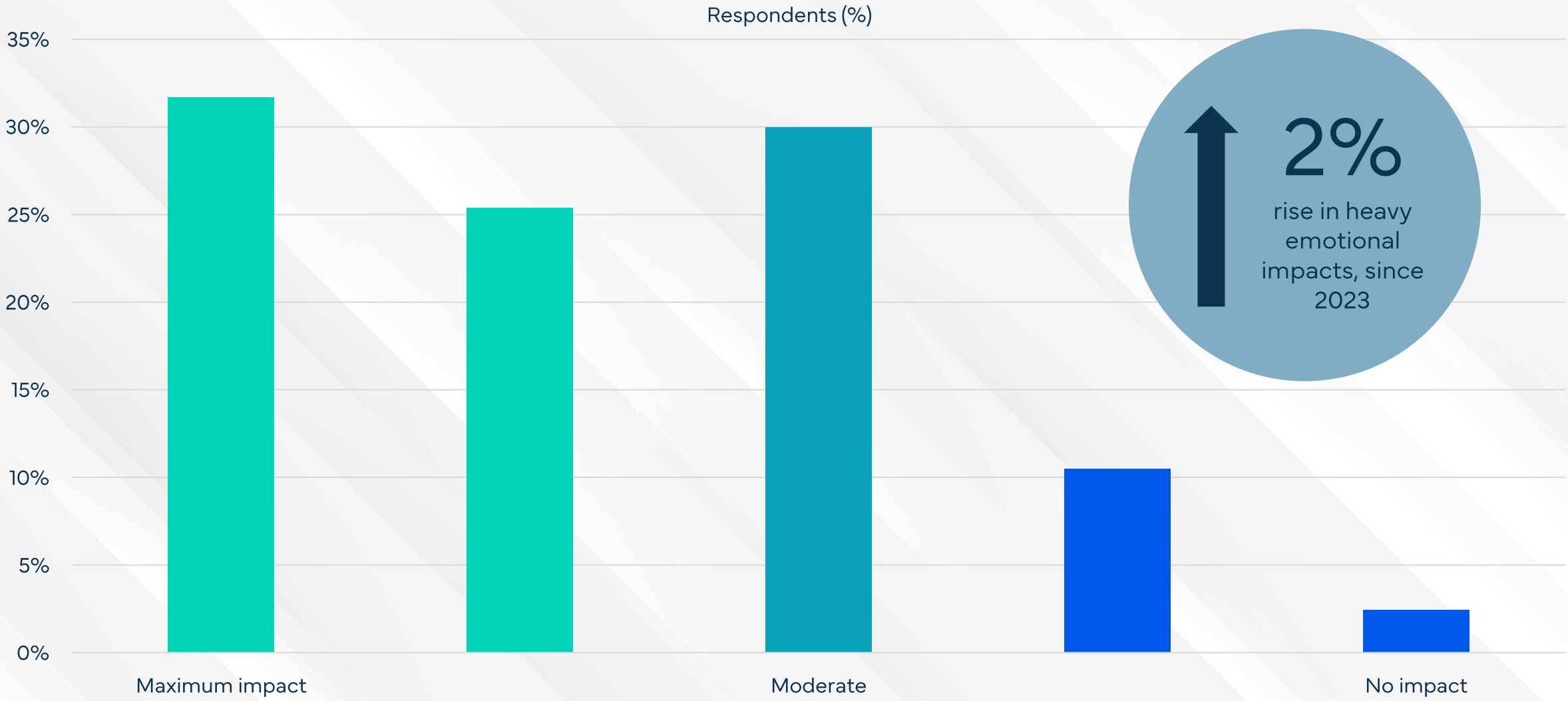
Only 2% of victims were able to fully recover their losses



25% did not try to recover their funds. 71% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

57% of the scam victims perceived a strong emotional impact

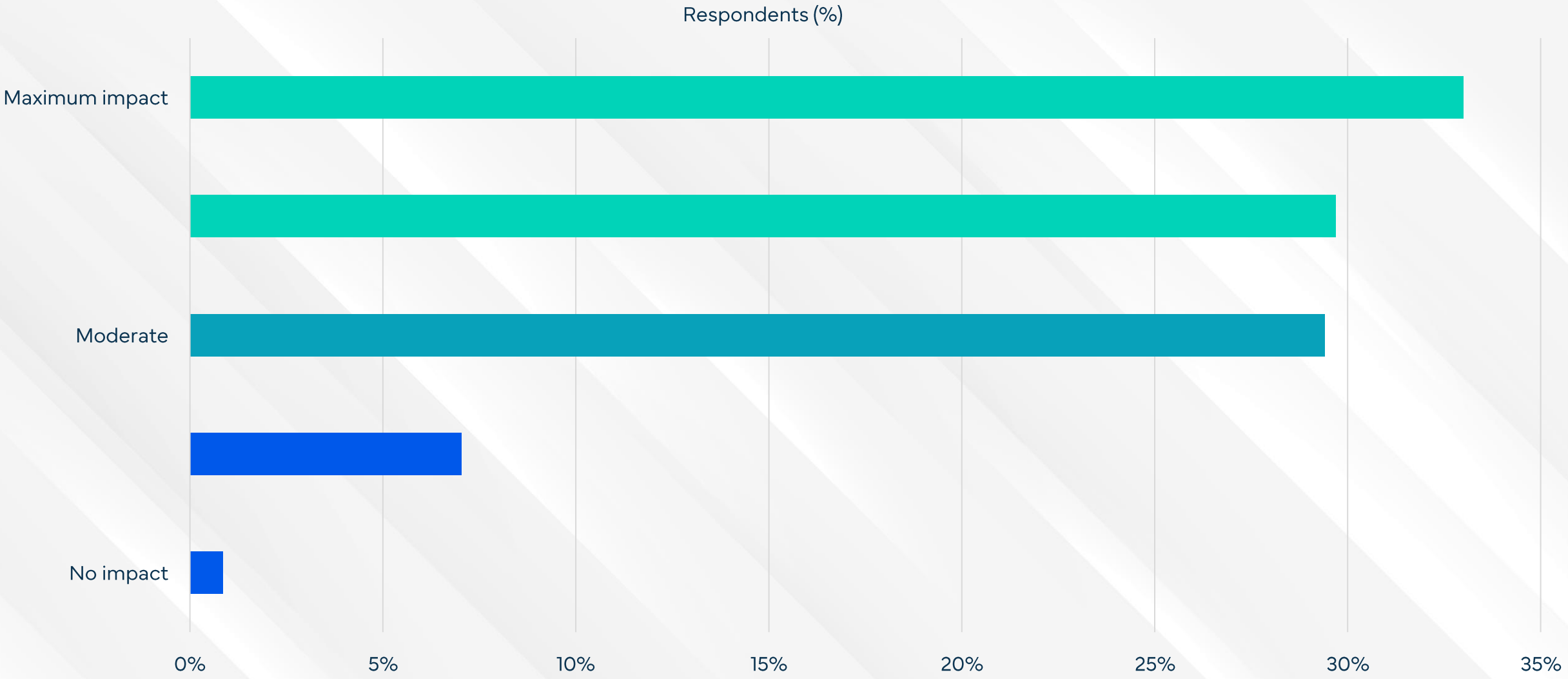


2%
rise in heavy emotional impacts, since 2023

13% of the survey respondents reported little to no emotional impact due to scams.

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

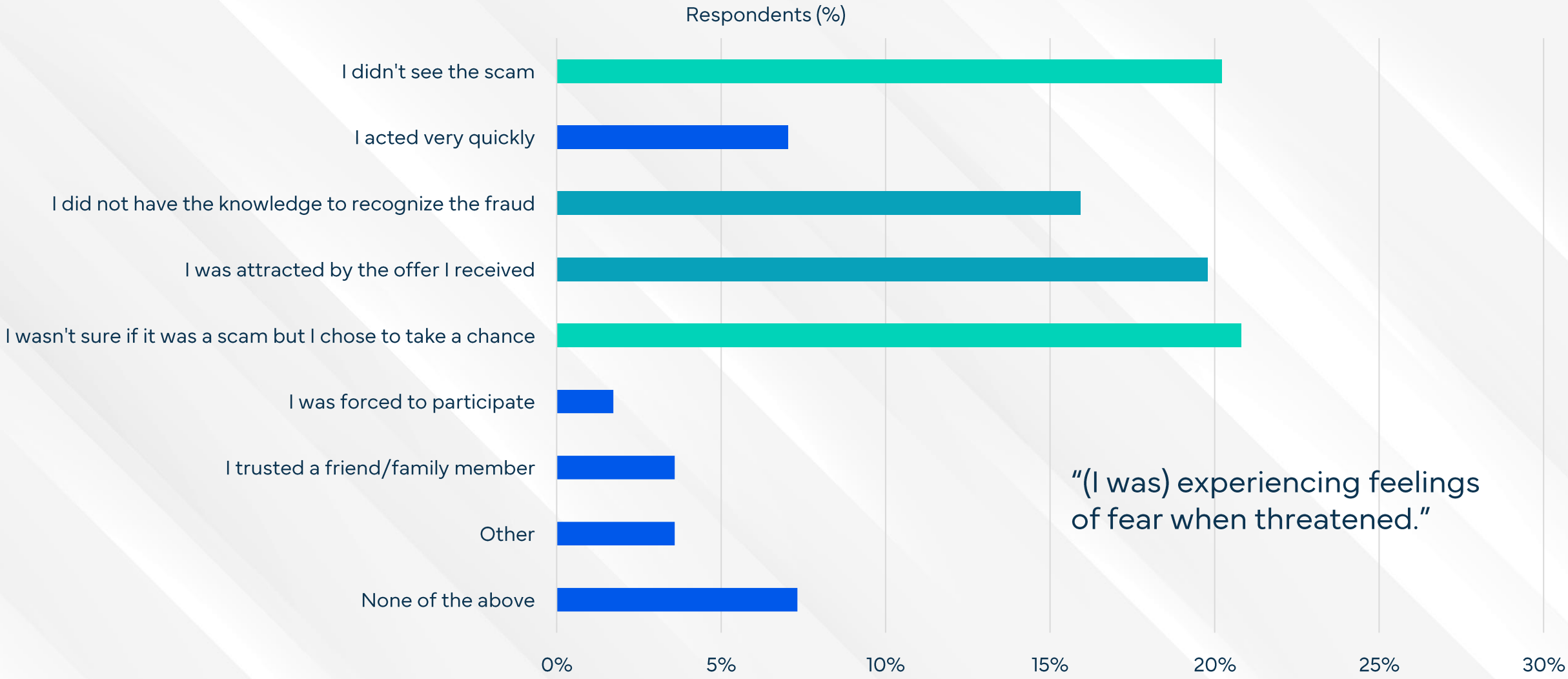
63% of Malaysians have less trust in the Internet as a result of scams



Only 8% of Malaysians 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?

Malaysians take risks despite being unsure whether they're facing a scam

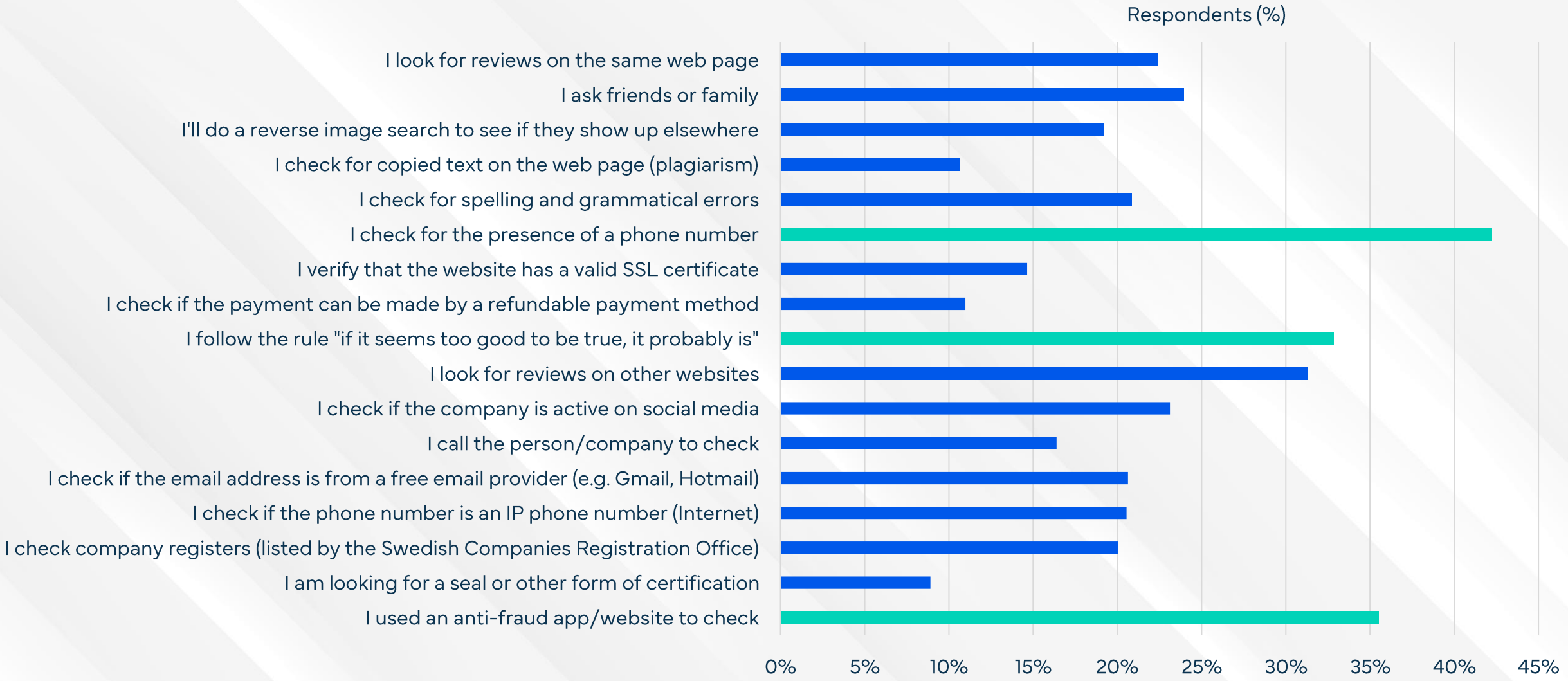


"(I was) experiencing feelings of fear when threatened."

Several victims also reported inability to see the scam while others were caught out by the offer.

Q19 - What was the main reason you were deceived?

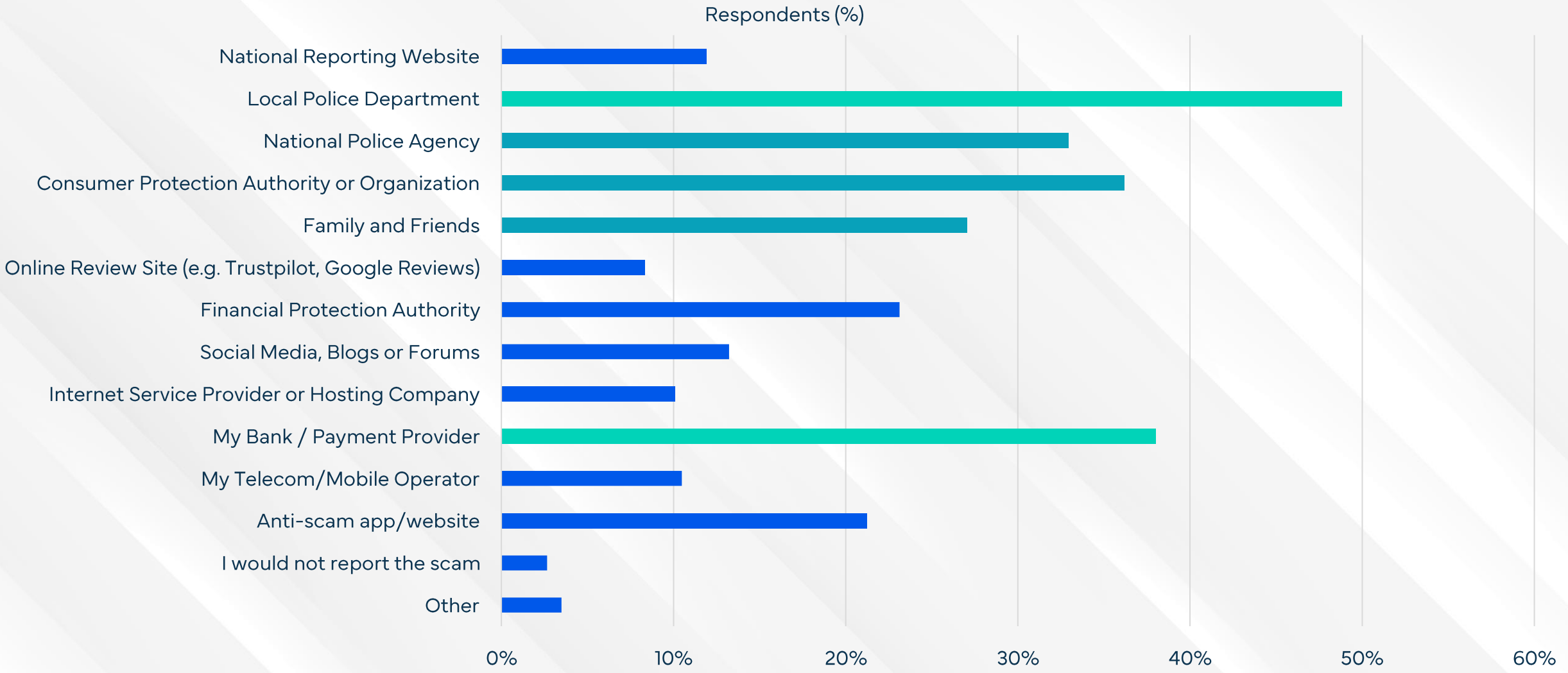
Nearly half of the participants check for the presence of a phone number



Many reported using anti-fraud apps/websites and following the “if it seems too good to be true” rule.

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

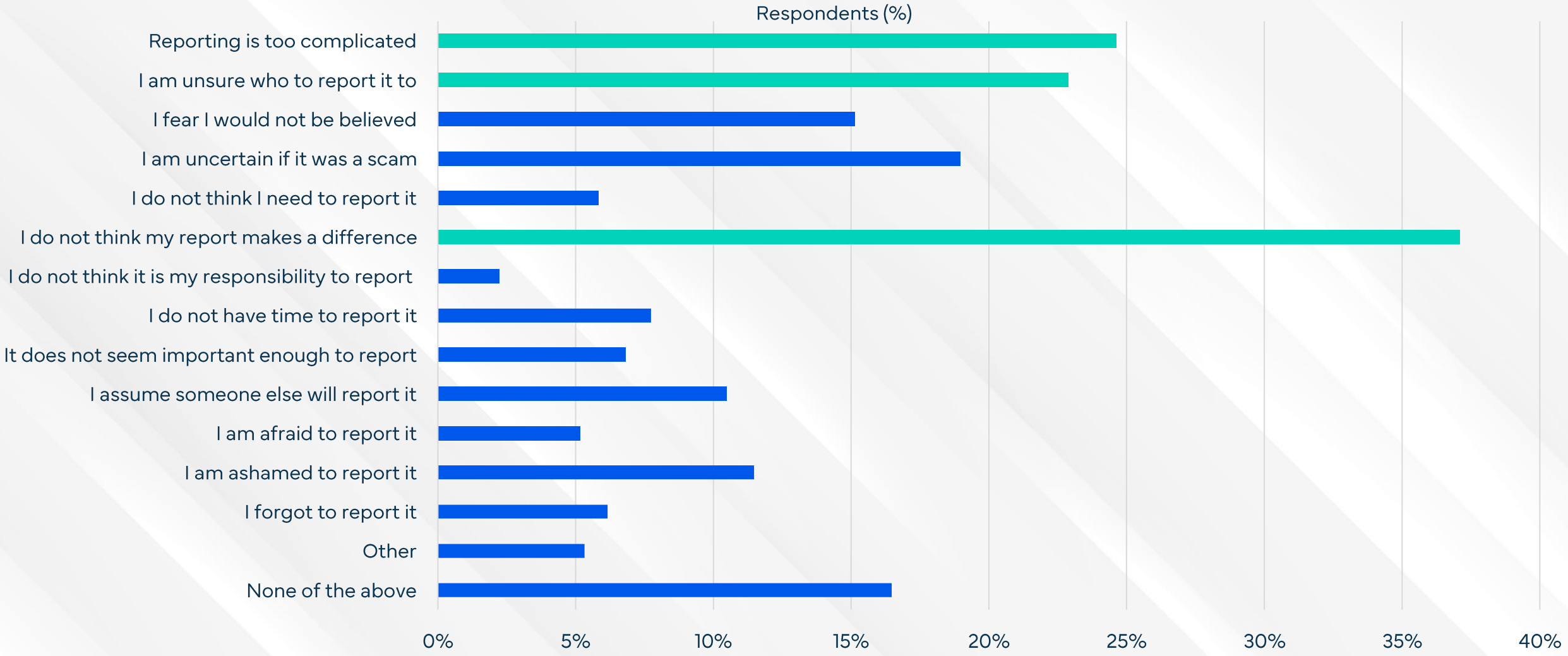
Scams are mostly shared with local law enforcement & banks



Consumer protection authority, national police, family/friends are popular places to report scams.

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

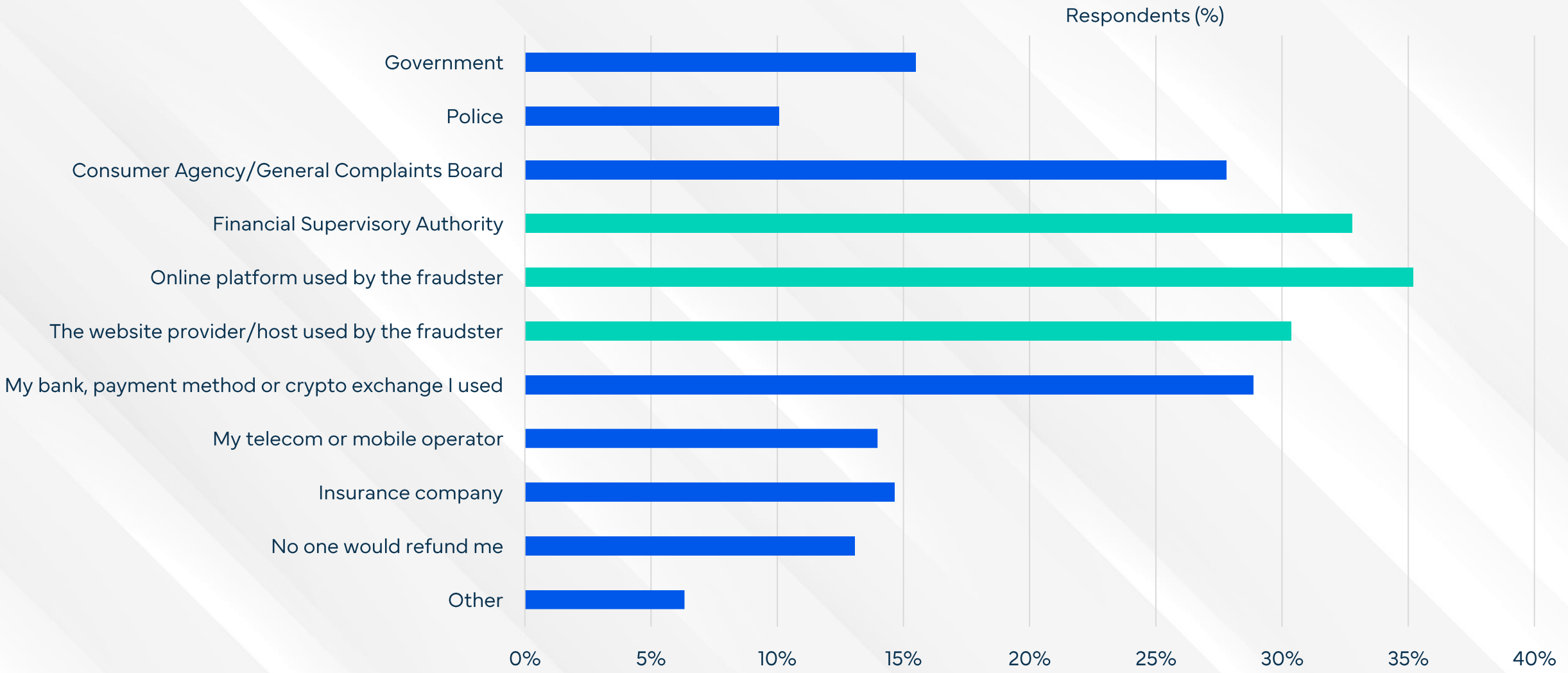
Many Malaysians assume reporting scams won't make a difference



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

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

13% of Malaysians assume no one will refund their scam losses



Others deem the online platform used, financial supervisory authority, and website host will refund them.

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

Citizens are unhappy with the Malaysia's attempts to arrest scammers

Overall, 26% of the participants rate the actions of the government as (very) bad, 34% as (very) good.

Q24 - Think about how well the government and other groups in your country are doing in the fight against online scams. How do you rate their efforts in the following categories?

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

"I will refuse (to be a money mule) while recording the conversation and report to the police."

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

Q25 - If someone offers you US$ 20,000 on the condition that you send US$ 19,000 to another bank account, leaving you with US$ 1,000 to keep, what would you do?

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

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.

Join the Network to Beat a Network

SCAMADVISER whoscall 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
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