SCAMADVISER

whoscall

The State of Scams in the Philippines 2024

GASA

Global Anti-Scam Alliance

Fraudsters target 1-in-3 as Filipinos lose $8.1 billion in 12 months

The 2024 State of Scams in the Philippines report, conducted by the **Global Anti-Scam Alliance (GASA)** in partnership with ScamAdviser and Whoscall, presents a detailed examination of the current scam situation in the Philippines. The survey, which includes responses from 1,000 Filipinos, sheds light on the increasing prevalence and sophistication of scams in the country.

According to the survey, **73% of Filipinos are confident in their ability to recognize scams**, reflecting a 5% increase in confidence compared to 2023. However, despite this growing awareness, **67% of Filipinos report encountering scams at least once per month**, an 8% increase in scam encounters per month since the previous year. Furthermore, half of Filipinos have faced more scam encounters in the past 12 months, signaling an upward trend in fraudulent activities.

Awareness of AI-generated scams is relatively high, particularly in relation to AI-generated text and images, though fewer Filipinos are familiar with complex AI-generated voice and video scams. Many scams are delivered via text/SMS messages and social media, with a significant **10% increase in text and SMS scams since 2023**. Platforms like Facebook and Gmail are among the most exploited by scammers, with Telegram, WhatsApp, and TikTok also being common channels for fraud.

A concerning finding is that **67% of Filipinos did not report scams to law enforcement**, despite 31% having done so. This underreporting suggests a lack of confidence in the effectiveness of authorities, with many Filipinos unsure if AI was used against them.

Shopping websites are identified as the most common type of scam in the Philippines, though 12% more people managed to avoid these scams compared to 2023. Despite this, the impact of scams remains significant, with 39% of survey participants losing money to fraud.

On average, **Filipino victims lost US$275 each**, contributing to a total estimated loss of **US$8.1 billion (459.98 billion PHP)**, which equates to 1.9% of the Philippines' GDP. This represents a 3% increase in scam losses since 2023. The report also highlights the speed at which scams are executed, with **76% completed within 24 hours of first contact**. Additionally, **67% of victims realized on their own that they had been scammed**, with others informed by family, friends, or online platforms.

Recovery of lost funds remains a significant challenge, with **only 3% of victims able to fully recover their losses**—a 2% decrease from the previous year. 72% of scam victims reported a strong emotional impact, a 7% increase since 2023, while 79% of Filipinos have lost trust in the Internet due to scams.

Filipinos often fall for scams due to attractive offers and acting hastily, with many victims admitting uncertainty about the legitimacy of the offers but choosing to risk it anyway. A large proportion of Filipinos check reviews before making decisions and following the rule of "if it seems too good to be true, it probably is."

Scams are mostly reported to local police stations and the national police agency, with anti-scam apps, websites, family, friends, and banks also being popular reporting destinations. However, many Filipinos do not report scams due to the complexity of the reporting process, a belief that reporting won't make a difference, and uncertainty about where to report. A notable **13% of Filipinos believe that no one will refund their scam losses**, while others expect the online platform used, the website provider, or consumer agencies to offer compensation. The survey also revealed dissatisfaction with the government's efforts to combat scams, with **23% of participants rating the government's actions as poor**, although 45% deemed them sufficient.

Disturbingly, **5% of Filipinos admitted they would consider being a money mule**, although 84% of those surveyed firmly stated they would refuse.

In conclusion, the State of Scams in the Philippines 2024 report reinforces the pressing need for enhanced preventive measures, stronger law enforcement, and more effective public awareness campaigns. The substantial economic and emotional impacts of scams highlight the critical importance of coordinated efforts to protect Filipinos and restore their trust in both digital platforms and governmental actions.

Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

The Philippines must invest in advanced scam detection technologies

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

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

Scams in the Philippines have reached an alarming level, 67% of Filipinos encounter scams monthly, an 8% rise compared to the previous year. Furthermore, the financial impact is substantial, with total scam losses reaching $8.1 billion (459.98 billion PHP), accounting for 1.9% of the country's GDP. This spike can be attributed to the growing sophistication of scam tactics, including the use of AI to deceive victims.

What types of scams have trended in the Philippines recently?

The most prevalent scams involve shopping websites, where scammers exploit consumers through fake online stores. Scammers also heavily rely on social media and messaging platforms, particularly Facebook, SMS, and instant messaging apps like WhatsApp. SMS scams have seen a 10% increase since 2023. Another emerging threat includes AI-generated scams, where scammers use AI to create scam text, images, and even complex voice and video content, though awareness of these sophisticated scams is still low.

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

The National Telecommunications Commission together with the Bangko Sentral ng Pilipinas released a directive to remove clickable links from SMS communications to prevent phishing attacks, demonstrating that detecting and blocking URLs in messages is an effective method for scam prevention.

Moreover, GoTyme Bank, a digital bank in the Philippines, has teamed up with trust technology companies as part of its commitment to fight against scams and fraud which is a definitive alignment with the vision of Whoscall to "Fight for a Scam Free Pilipinas". These collective efforts underscore the country's dedication to creating a safer digital environment for its citizens.

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

To effectively combat scams, sectors such as government, banks, and telecoms should work to educate and provide tools for consumers to protect themselves. The implementation of more real-time scam detection tools, particularly within banking systems, is essential to identifying scam activities before they lead to financial loss. In addition, increasing public awareness through educational campaigns is important, but this effort must be complemented by simplified reporting mechanisms and stronger collaboration between telecom companies, banks, and online platforms. Additionally, encouraging organizations to invest in advanced scam detection technologies is essential to counteract the evolving tactics used by scammers.

Aaron Chiou
Product Director

SCAMADVISER

“Fight for a Scam Free Pilipinas” with Mel T. Migriño of Gogolook

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 this Philippines 2024 State of Scams, GASA interviewed **Mel Migrino, SEA Regional Director** and **Philippines Country Head** of **Gogolook**.

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

In the prior years, scams in the Philippines were more of an enterprise- to- consumer issue. Most of the scams in the social media channels and sellers offering fake items in online shopping platforms. Most of the scam cases revolve around shopping and payment scams.

With CICC at the helm in fighting against scams, the issue of the growing cases of scams has become a national concern as Filipinos have been victimized regardless of his/her social economic status. We have seen how scam strategies progressed to proliferate human trafficking in the country and within ASEAN.

As this is a problem not only recognized by the government but also the business enterprises where they face numerous complaints from their customers asking for their money to be returned. A greater majority of the scam cases in the country cannot be recovered due to lack of infrastructure to detect, block and prevent. Hence, the combined effort to educate and digitally enable Filipinos is crucial towards the continued uptake of digital transformation in the country.

What types of scams have trended in the Philippines recently?

With approximately 87M Filipinos on the internet and consuming about 8-9 hours every day on social media and digital channels, there is no doubt that Filipinos look at technology as a lifestyle enabler.

As Filipinos get more and more engaged on digital platforms, the techniques and tactics of scammers also scale faster. The most common types of scams in the Philippines for the past 2-3 years are the Shopping Scams, Identity theft, Investment Scams which are sometimes rooted from relationship or love scams and job scams.

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

The Philippine government has designated the Cybercrime Investigation and Coordinating Center (CICC) to develop programs to fight against scams and fraud in the country. It is supported by its national movement to fight against scams by educating Filipinos through the appointment of Scam Watch Pilipinas. Both entities are strategic partners of Gogolook in the Philippines to enable Filipinos to safely navigate the digital space with confidence.

Among the key programs are:

- community reporting of scam numbers in 1326 hotline of Inter-Agency Response Center (IARC) and Whoscall community reporting which enable the private-public partnership of Gogolook and the Philippine Government to identify and block the scam numbers and URLs.
- the passage of Republic Act No. 12010 or the Anti-Financial Account Scamming Act (AFASA) to protect consumers against financial related cybercrimes
- the anti-scam educational campaigns to the academe and local government units that reach the grassroots in Metro Manila and provincial areas
- the promotion of the Check with SEC tool so that consumers and enterprises can identify if the other party is fictitious or legitimate
- continuous monitoring and response of the CICC on scam or fraudulent related incidents on unregistered mobile numbers used to commit scams and fraud which are outliers of the implementation of the SIM Registration Act.

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

It is good to see that there have been notable efforts initiated by the government agencies, Non-Profit Companies and business enterprises. The missing piece is the enactment and implementation of the Anti-Financial Account Scamming Act (AFASA) as this will provide governance and legal authority in combating financial cybercrimes and protect the interest of the consumers. Once this is fully approved, everything else will follow in a more defined fashion.

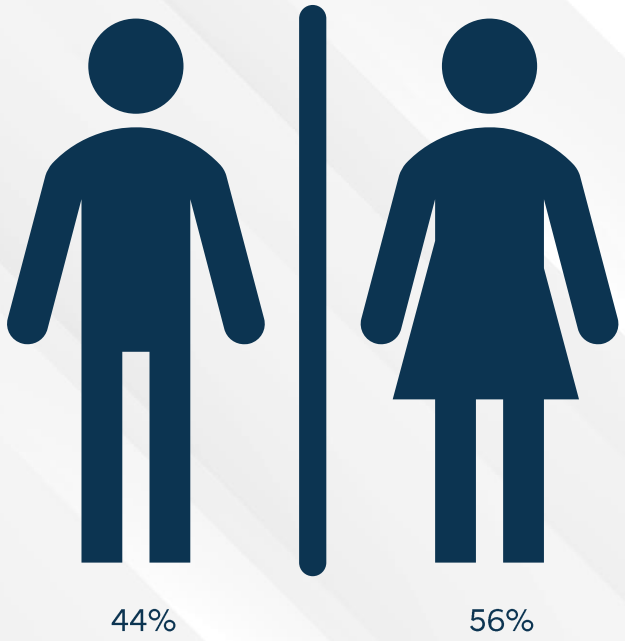
Mel T. Migriño
SEA Regional Director &
Philippines Country Head
Gogolook

1,000 Filipinos completed the State of Scams survey

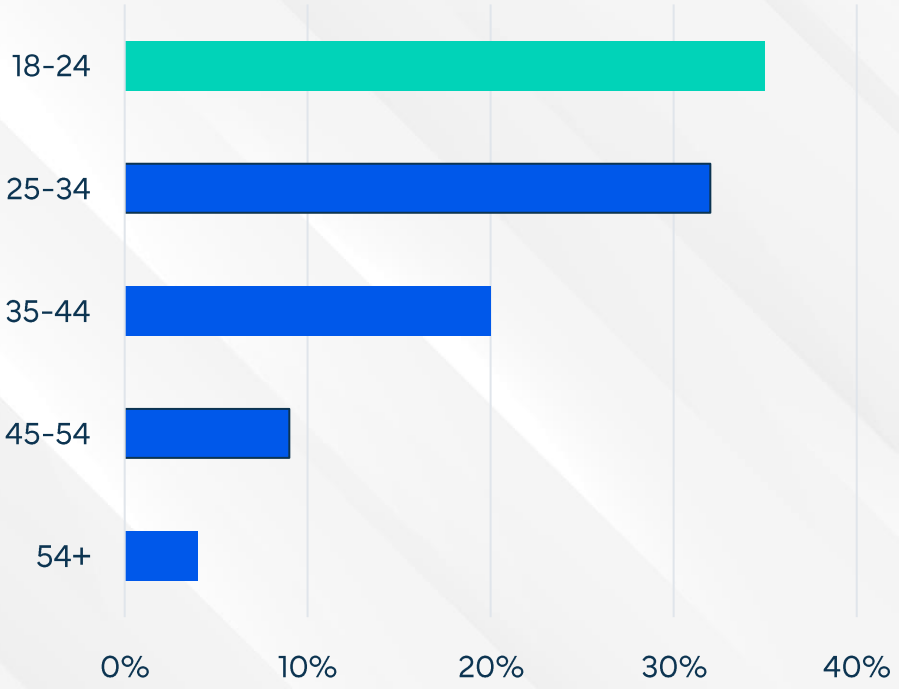
SCAMADVISER whoscall

GASA Global Anti-Scam Alliance

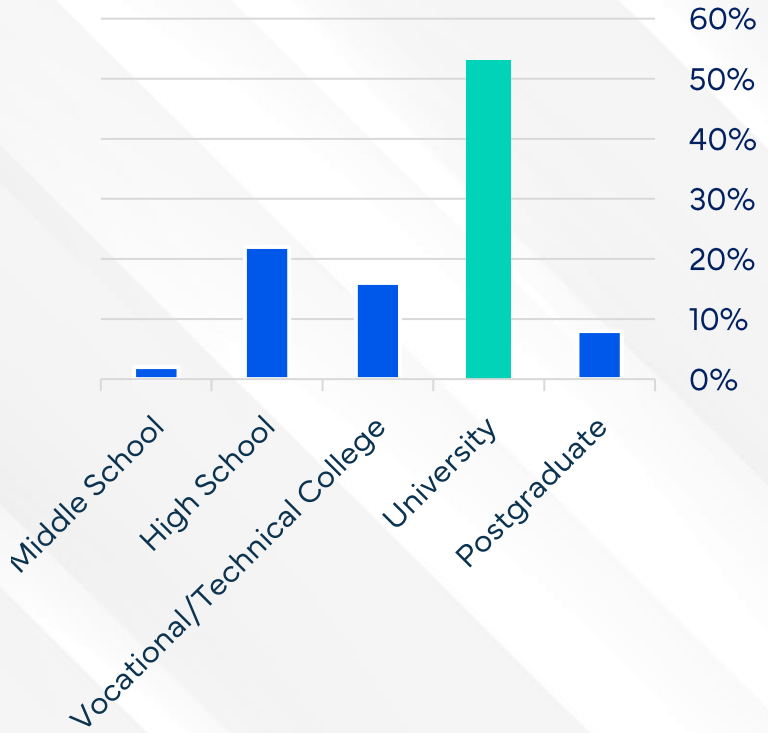
Gender



Age Range

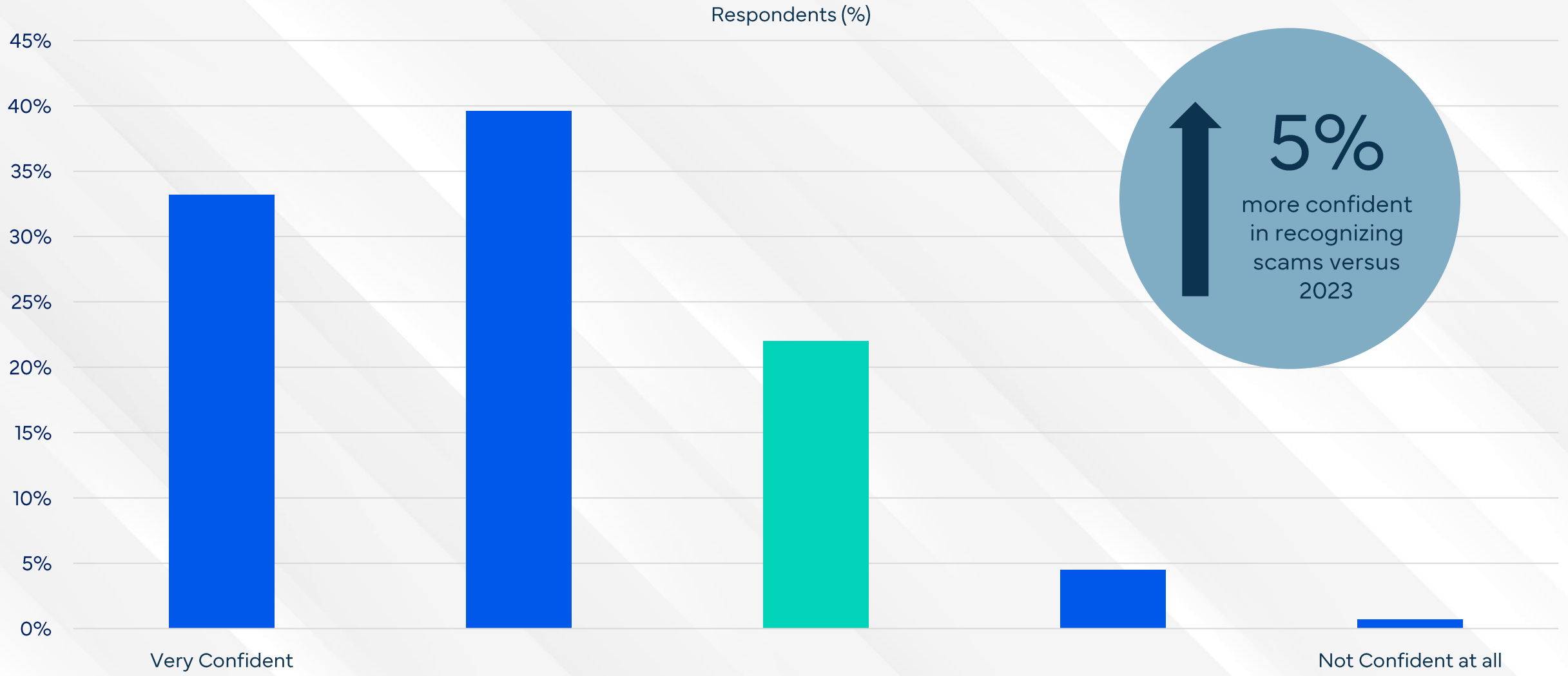


Education



The demography of respondents to the State of Scams in the Philippines 2024 survey consists of more men than women. A large proportion were between 18-24 of age, university degree.

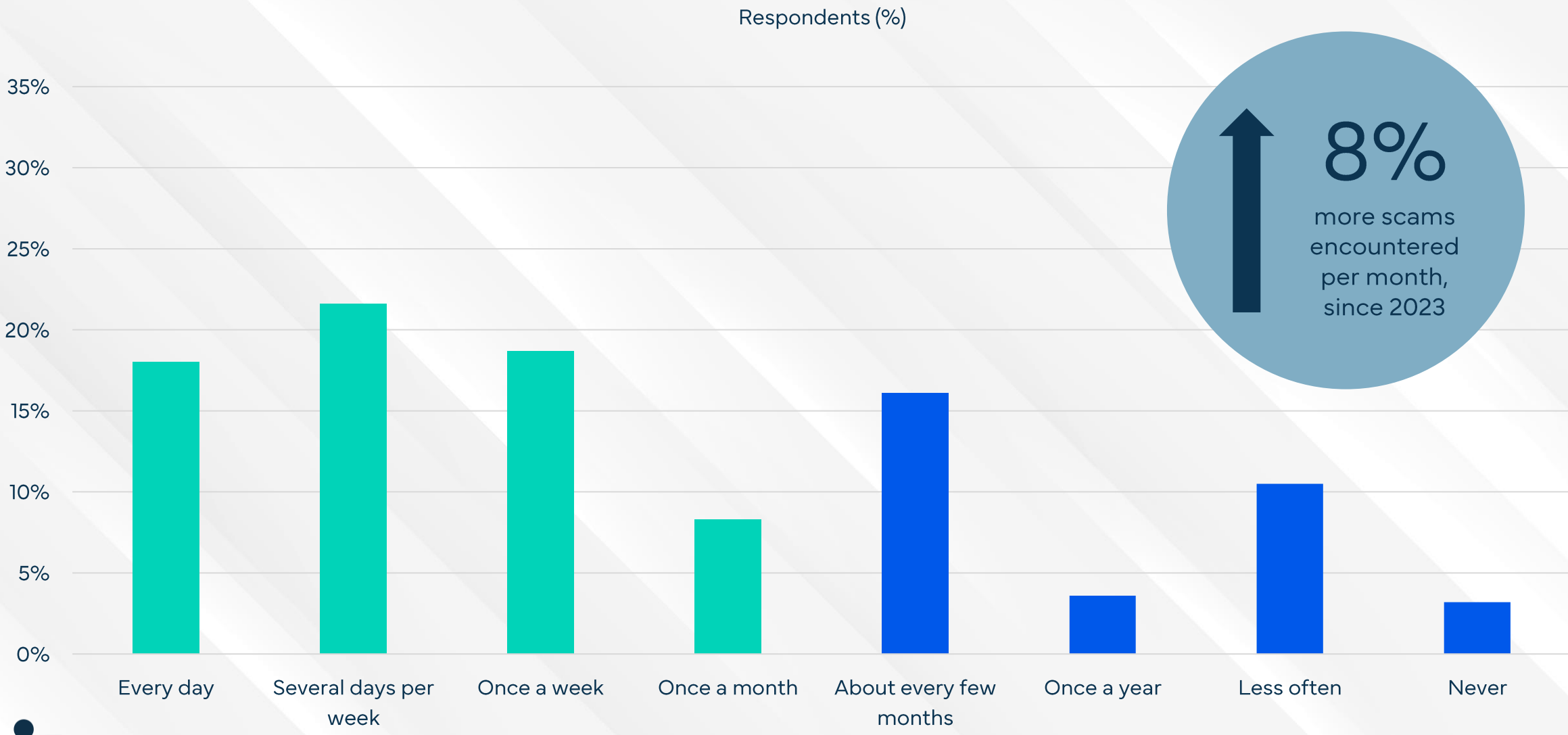
73% of Filipinos are confident in their ability to recognize scams



Only 5% of respondents are not (very) confident in recognizing scams, at all.

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

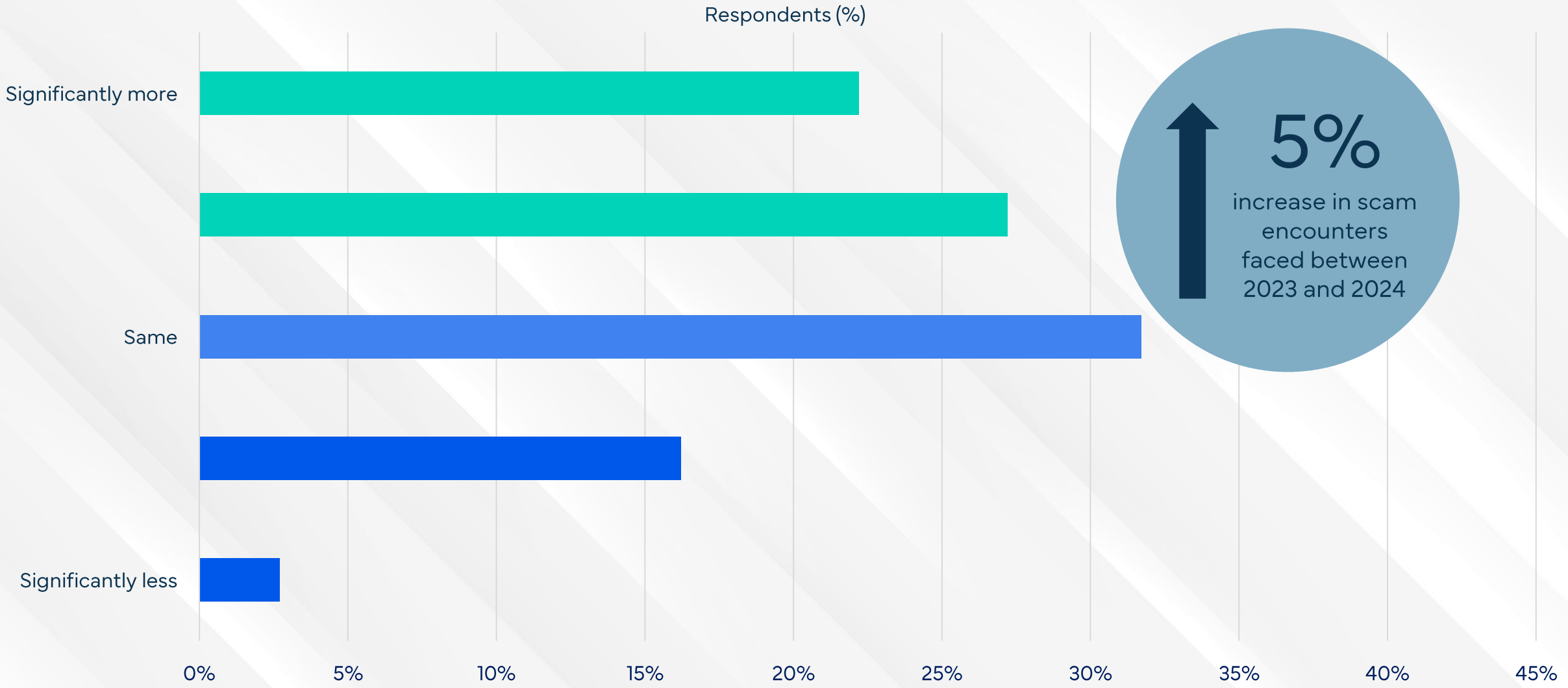
67% of Filipinos encounter scams at least once per month



14% of Filipino respondents encountered scams lasting more than year.

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.

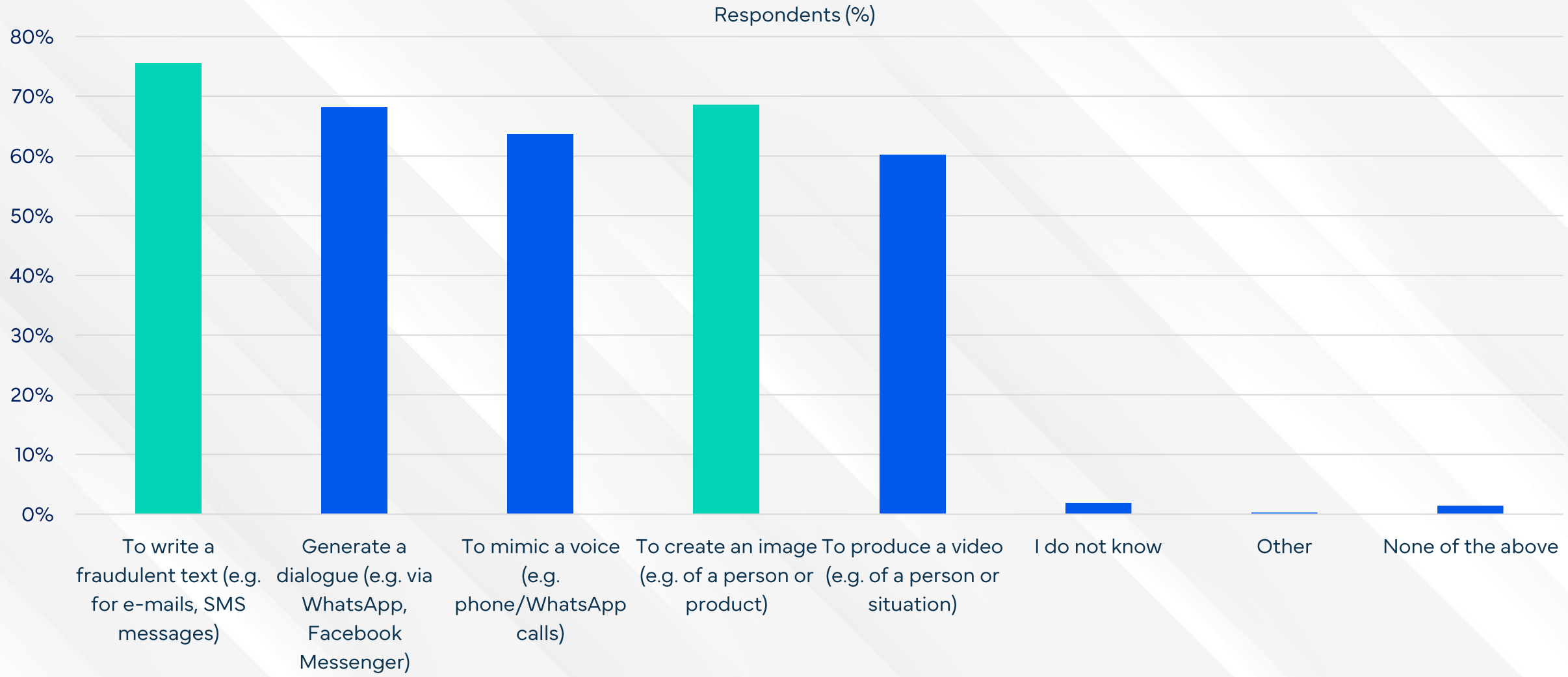
49% of Filipinos faced more scam encounters in the last 12 months



Only 19% of Filipino 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?

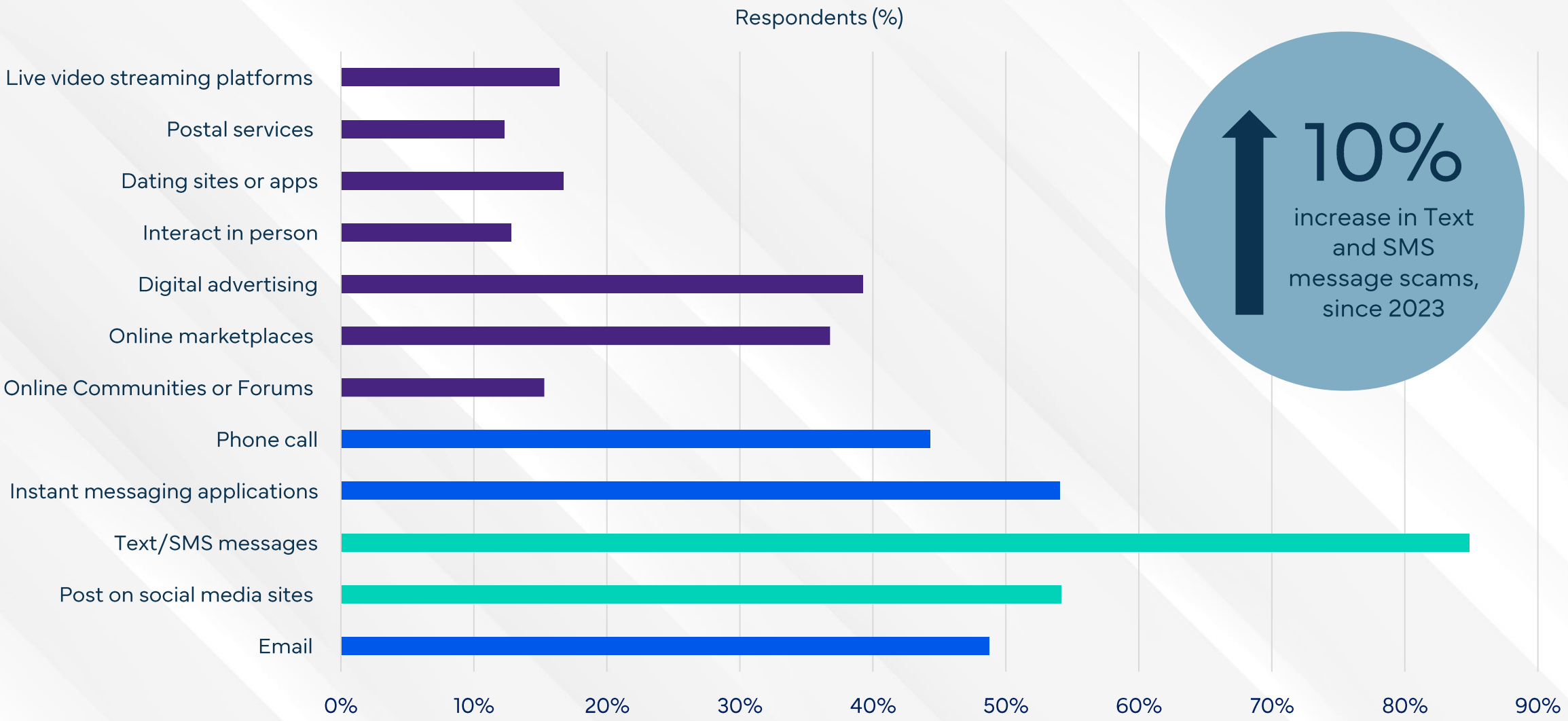
Most Filipinos are aware scammers can use AI against them



Awareness of AI generated text & images is high, while complex voice & 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 & social media

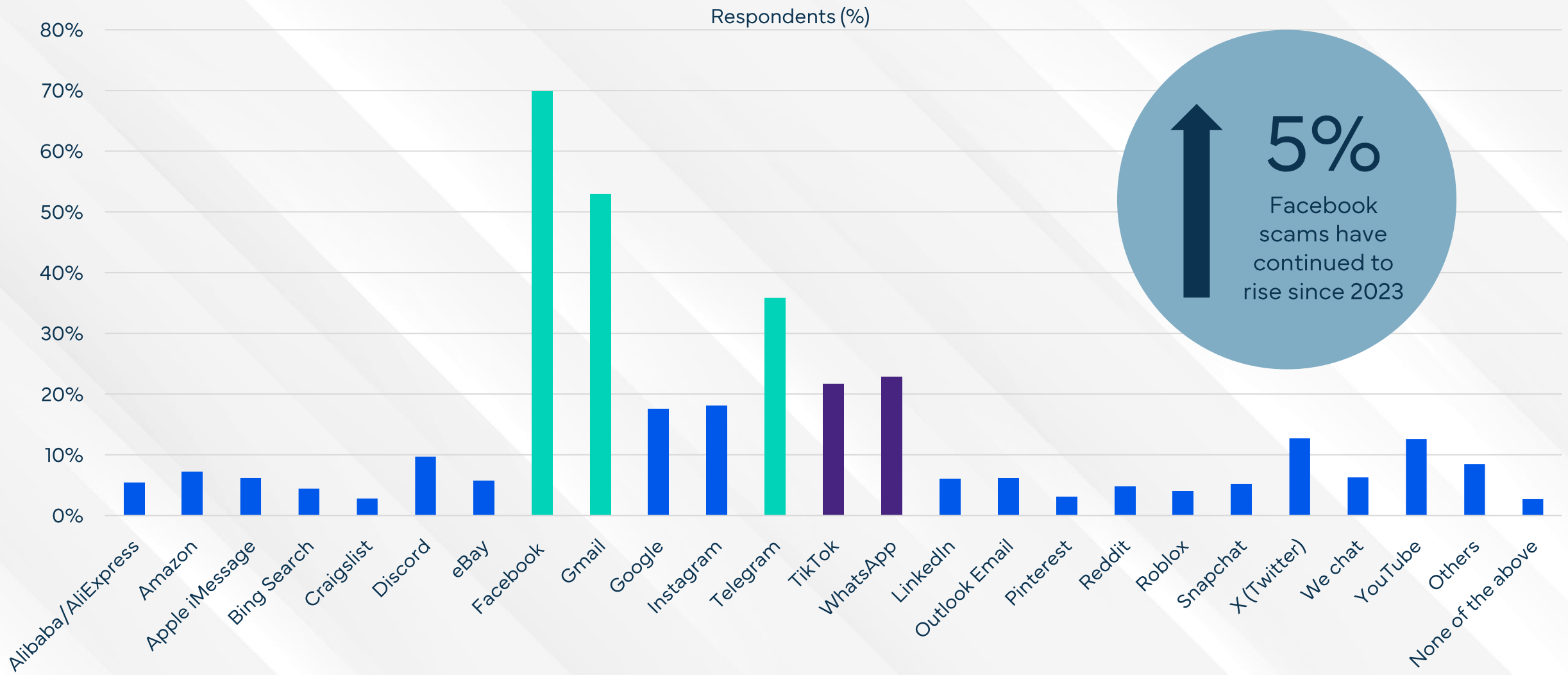


10%
increase in Text and SMS message scams, since 2023

Instant messaging apps, emails, & phone calls are also common scam media.

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

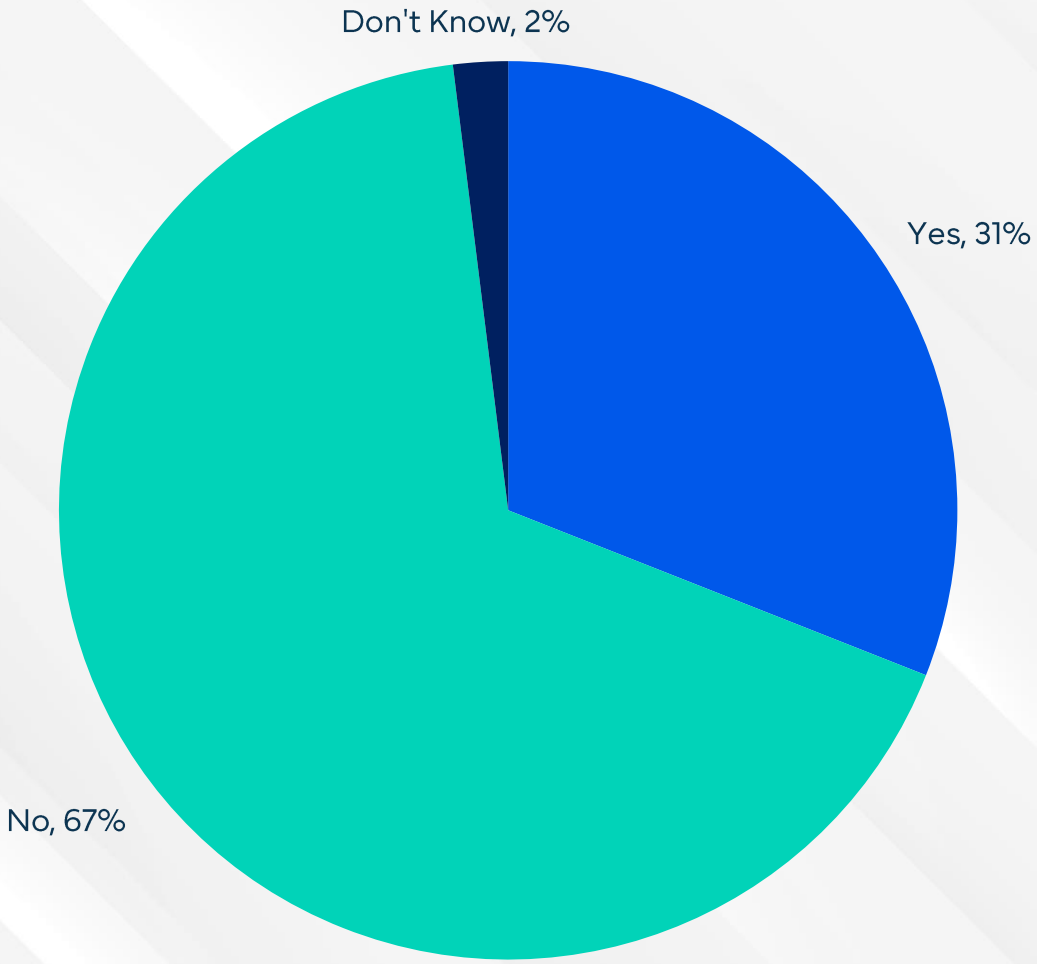
Facebook and Gmail are the platforms most exploited by scammers



Telegram, WhatsApp and TikTok round out the top five platforms where people encounter scams.

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

67% of Filipinos did not report the scam to law enforcement



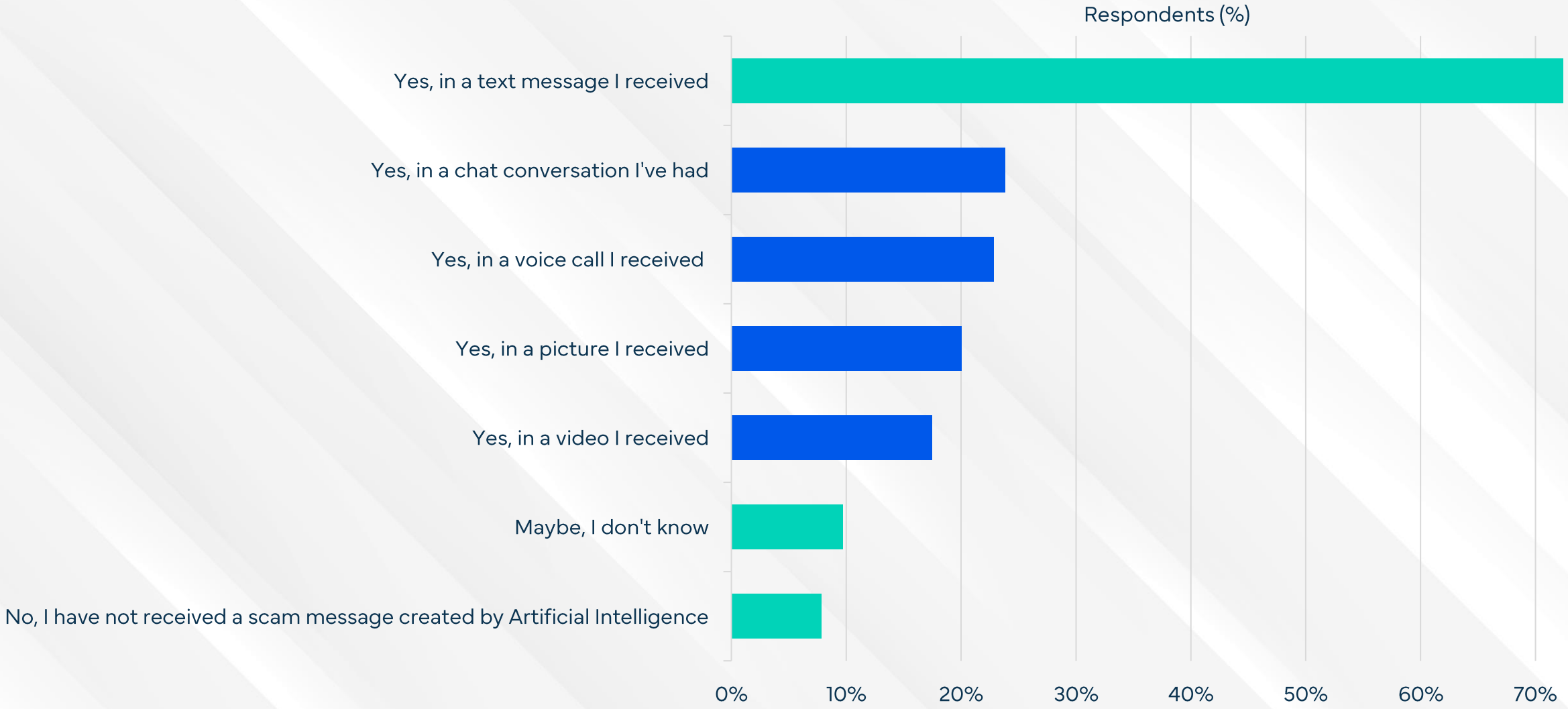
5%

more Filipinos don't report scams to law enforcement

31% 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?

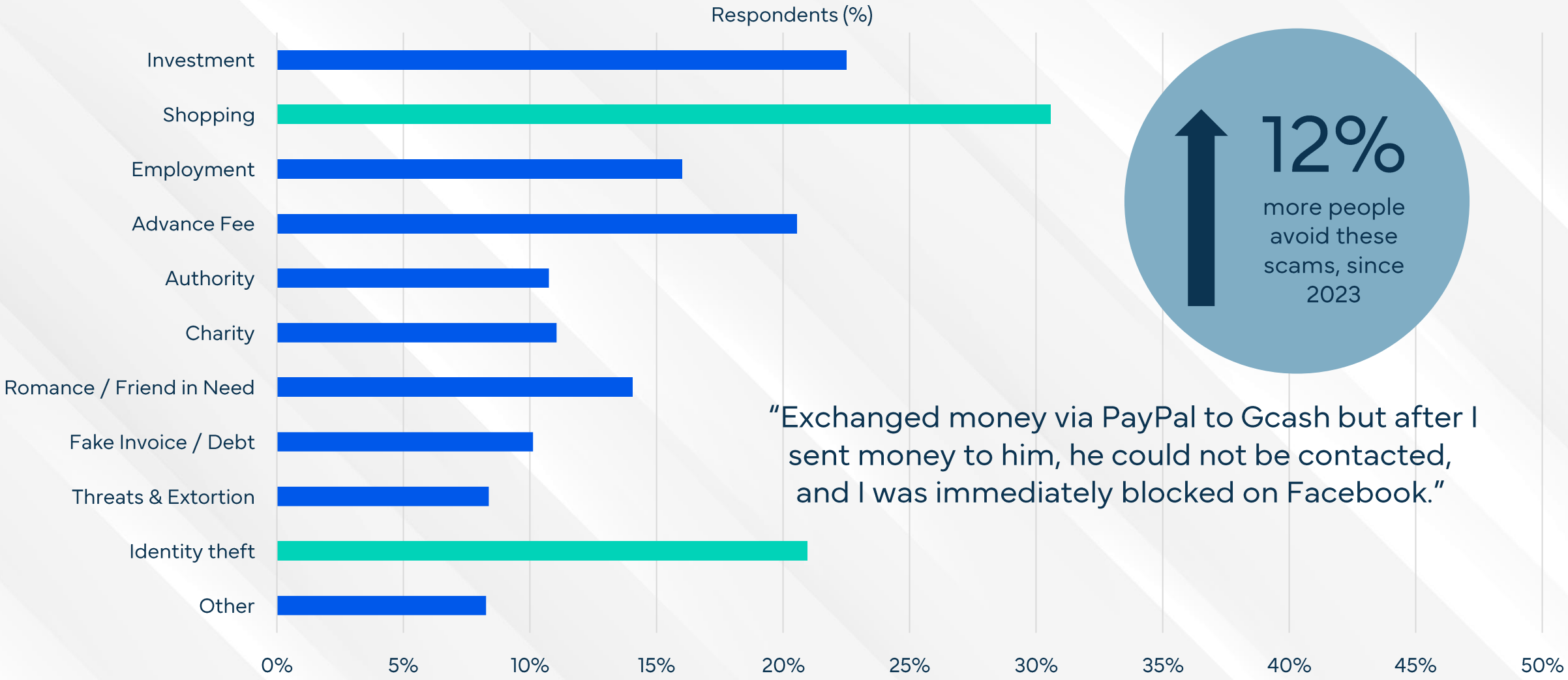
10% of Filipinos are uncertain whether AI was used to scam them



8% of Filipinos 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 websites are the most common type of scam in the Philippines



12%
more people avoid these scams, since 2023

"Exchanged money via PayPal to Gcash but after I sent money to him, he could not be contacted, and I was immediately blocked on Facebook."

17% did not fall victim to the most common scams in the last year. 1.73 scams were reported per victim.

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

The Philippines scam victims share their stories

SCAMADVISER whoscall

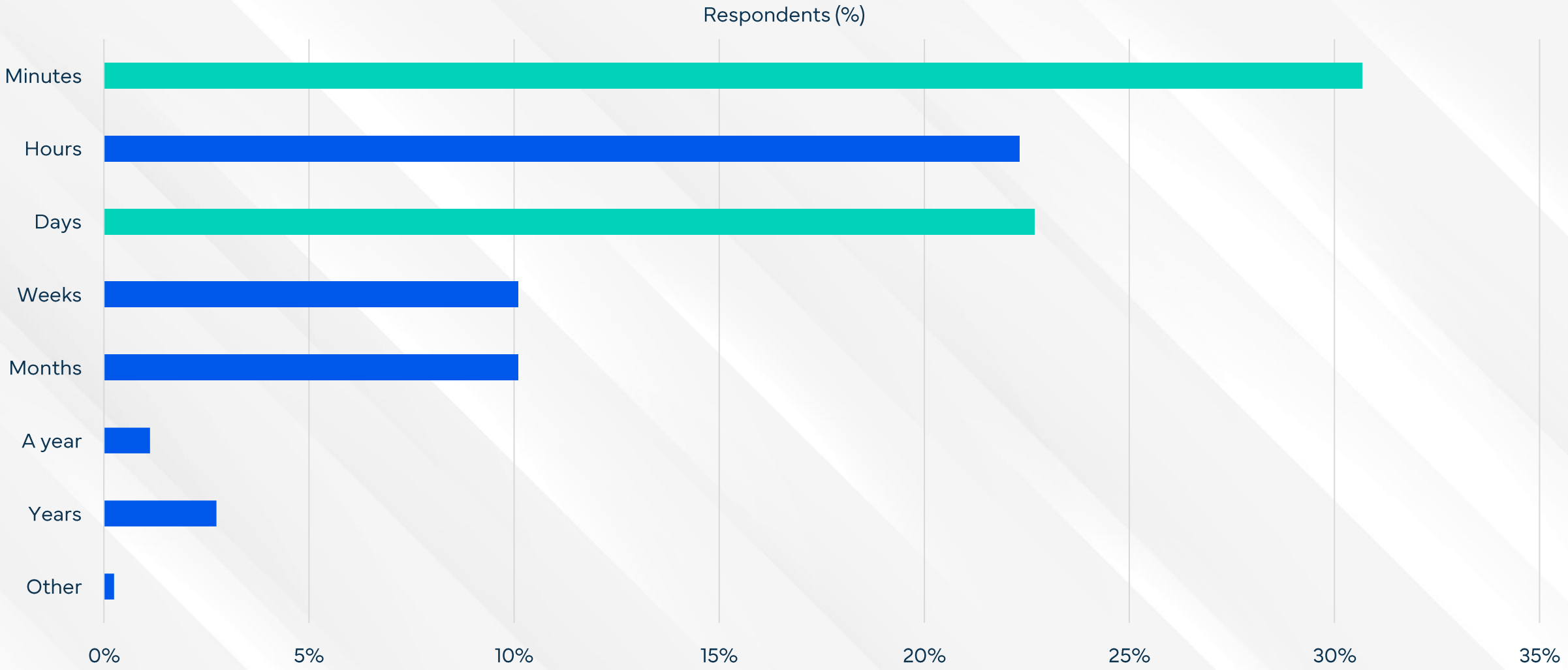
GASA Global Anti-Scam Alliance

"My friend on Facebook asked for money to support a charity for persons with disability (PWD). I thought it was really for a charity and (contributed) but I later found out that he was just collecting money for personal needs."

"I was scammed on a website that I thought would make my money grow, but at first I was able to cash out but when I reinvested, it turned out that I could (not) cash out because the requested amount was getting bigger and bigger and that's when I realized that I was scammed."

"Someone texted me saying I won a prize from Netflix. That they would send a code to me and I would need to send the code back to them to verify. It turns out that was the OTP needed to open a Netflix account in my name and on my Globe Account. I realized this immediately and changed the password for the newly created Netflix account. I tried to ask globe to reverse the charge to no avail."

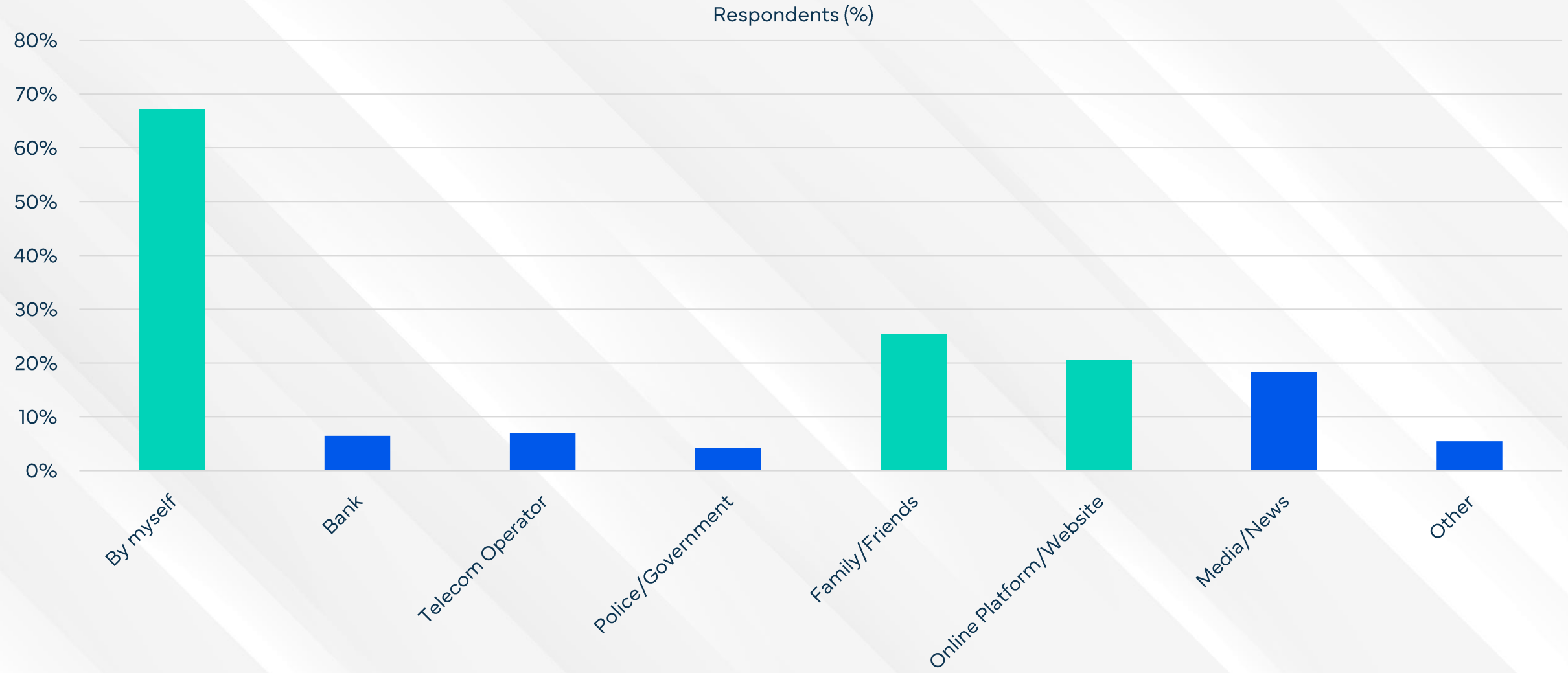
76% of scams are completed within 24 hours of first contact



31% reported scams that were over in minutes, while 4% 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?

67% came to their own conclusion that they had been scammed

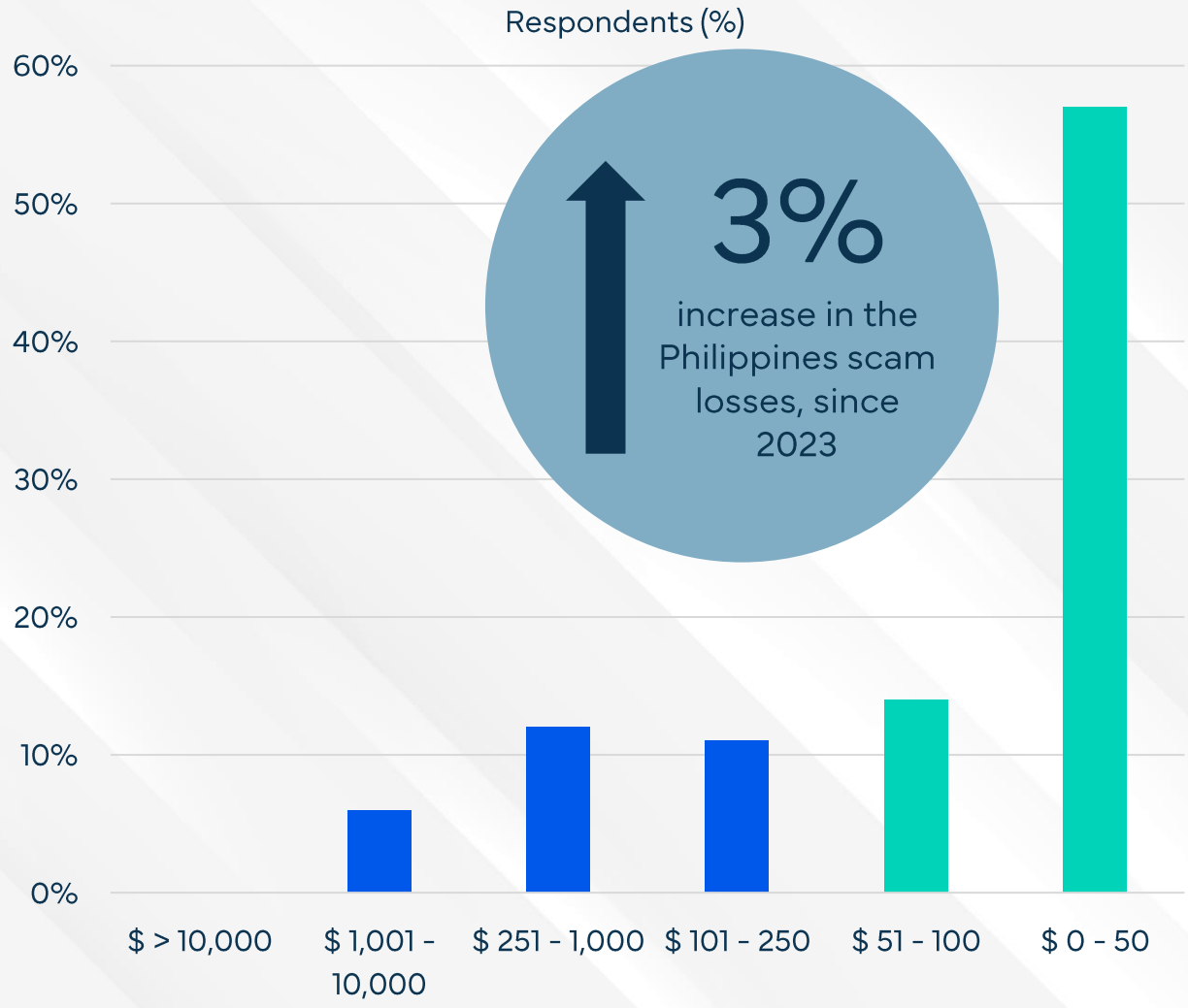


Others were informed by family/friends while online platform/sites are also key in pointing out scams.

Q13 How did you discover you were scammed?

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

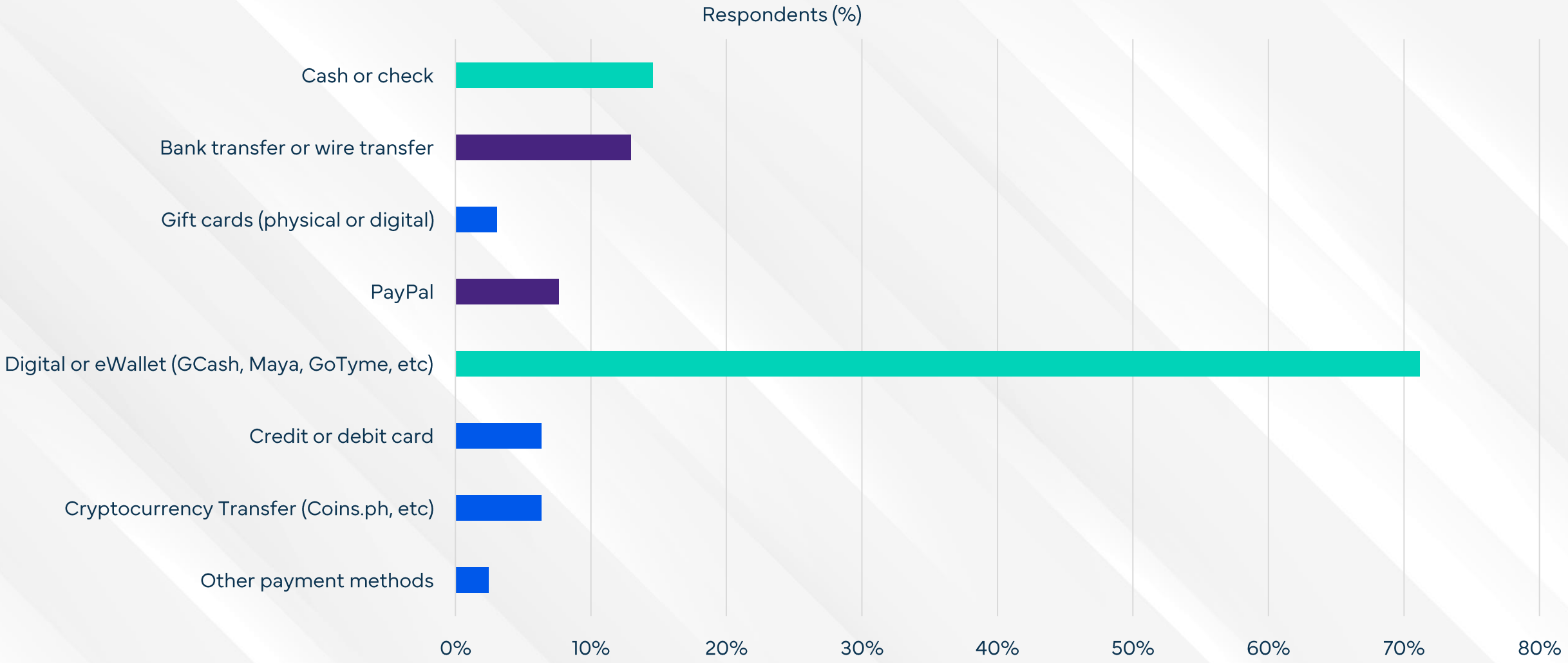
Survey Key Statistics	
Persons approached	1,578
Participants completing the survey	63%
Participants losing money	617
% losing money / approached persons	39%
Average amount lost in US Dollars	275
Total country population	118,277,063
Population over 18 years	75,701,616
# of people scammed > 18 years	29,603,465
Total scam losses (USD)	8,140,952,920
Total scam losses (PHP)	459,977,434,309
Gross Domestic Product (USD, millions)	435,675
% of GDP lost in scams	1.9%



In total, the Philippines lost $8.1 billion to scams, which is equal to 1.9% of the Philippines's GDP.

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

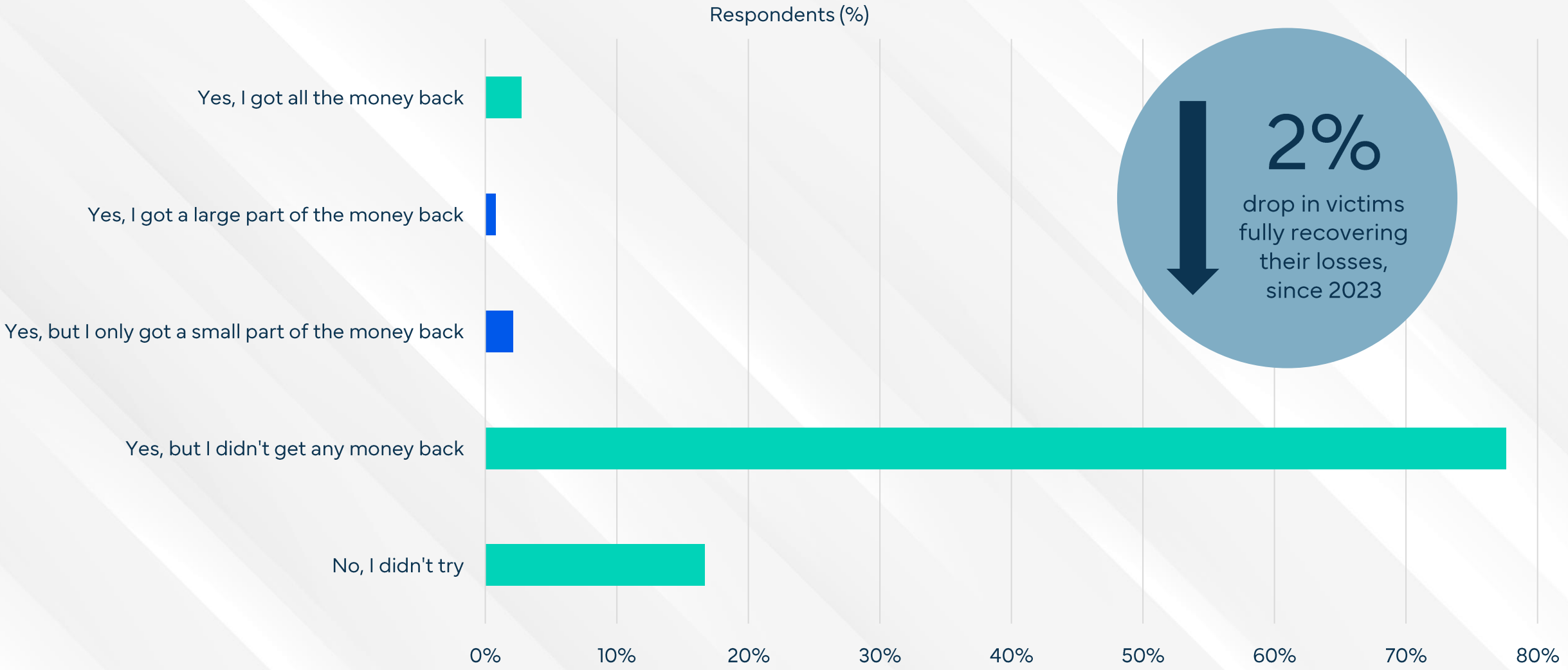
Digital/e-wallets are the dominant scam payment method



Cash, check & wire transfers are also popular tools which scammers use to receive their stolen gains.

Q15 - How did you pay the scammer?

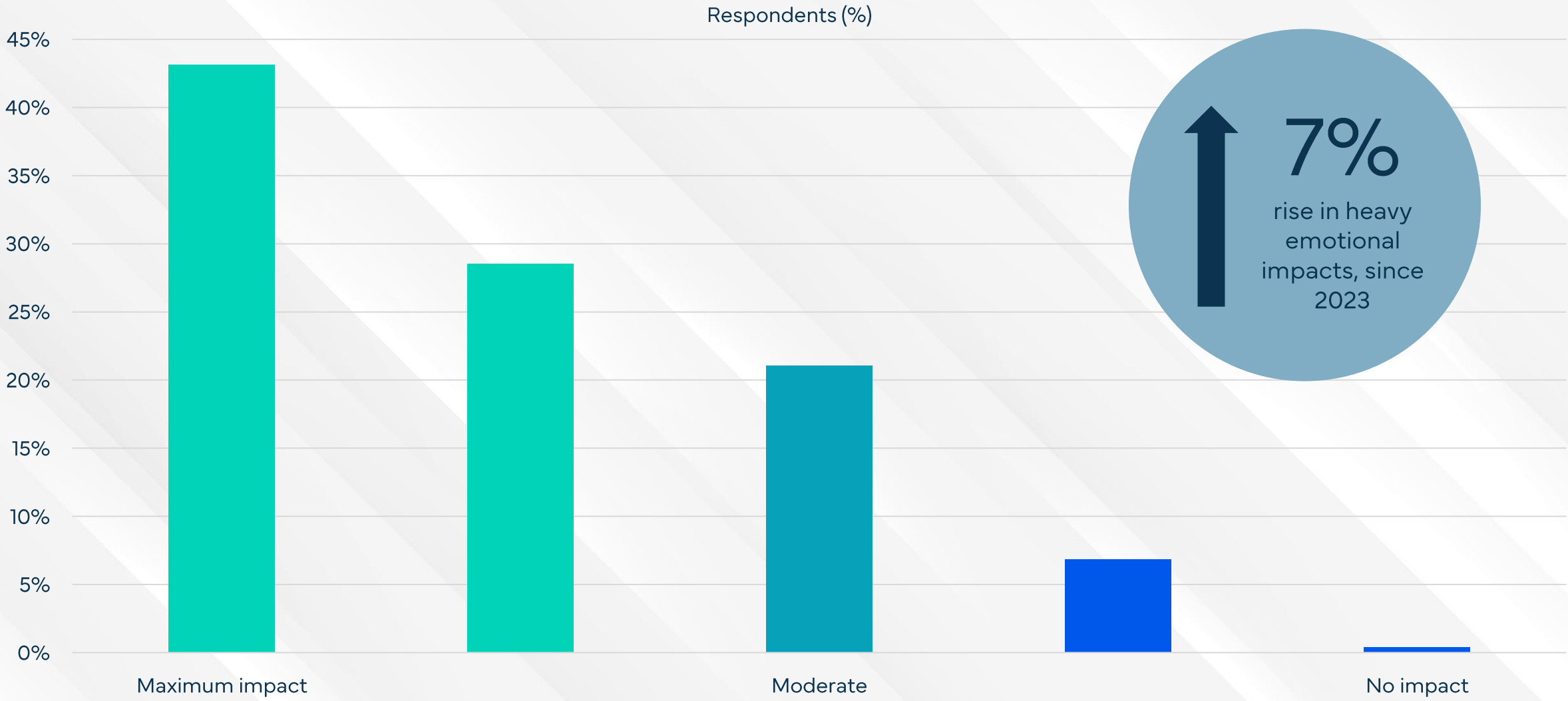
Only 3% of victims were able to fully recover their losses



17% did not try to recover their funds. 78% tried but were not able to recover any money.

Q16 - Did you try to recover the money lost?

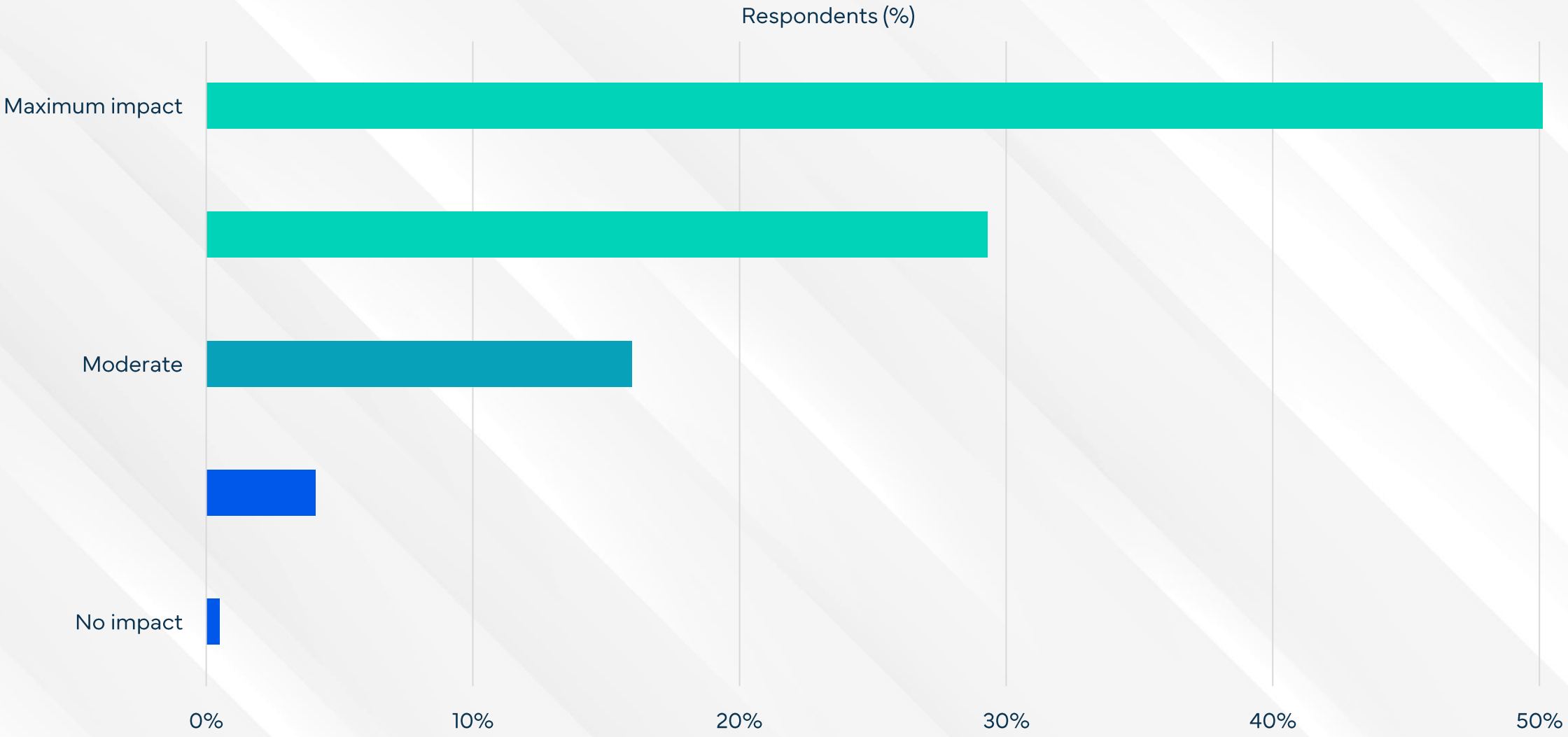
72% of the scam victims perceived a strong emotional impact



7% of the survey respondents reported little to no emotional impact due to scams.

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

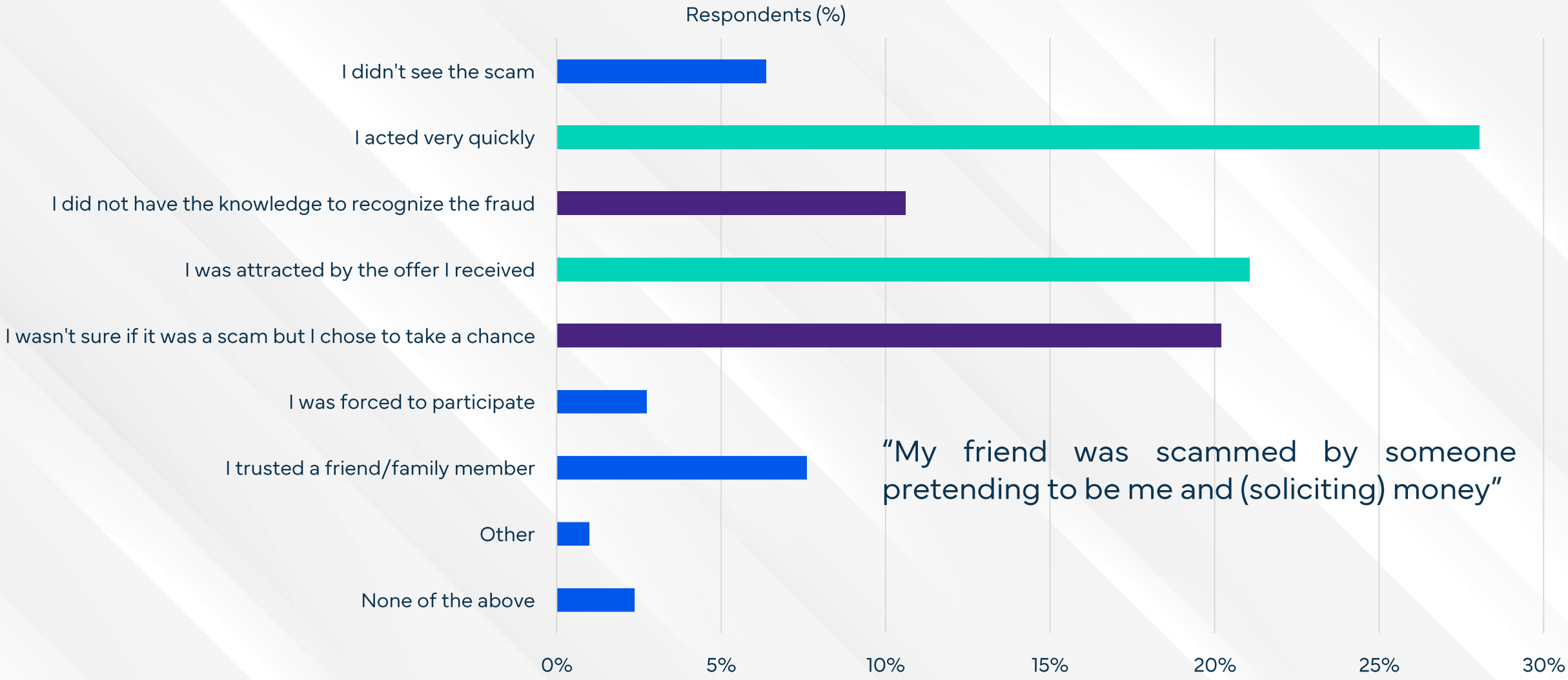
79% of Filipinos have lost trust in the Internet as a result of scams



Only 5% of Filipinos 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?

Filipinos fall for attractive offers by acting hastily

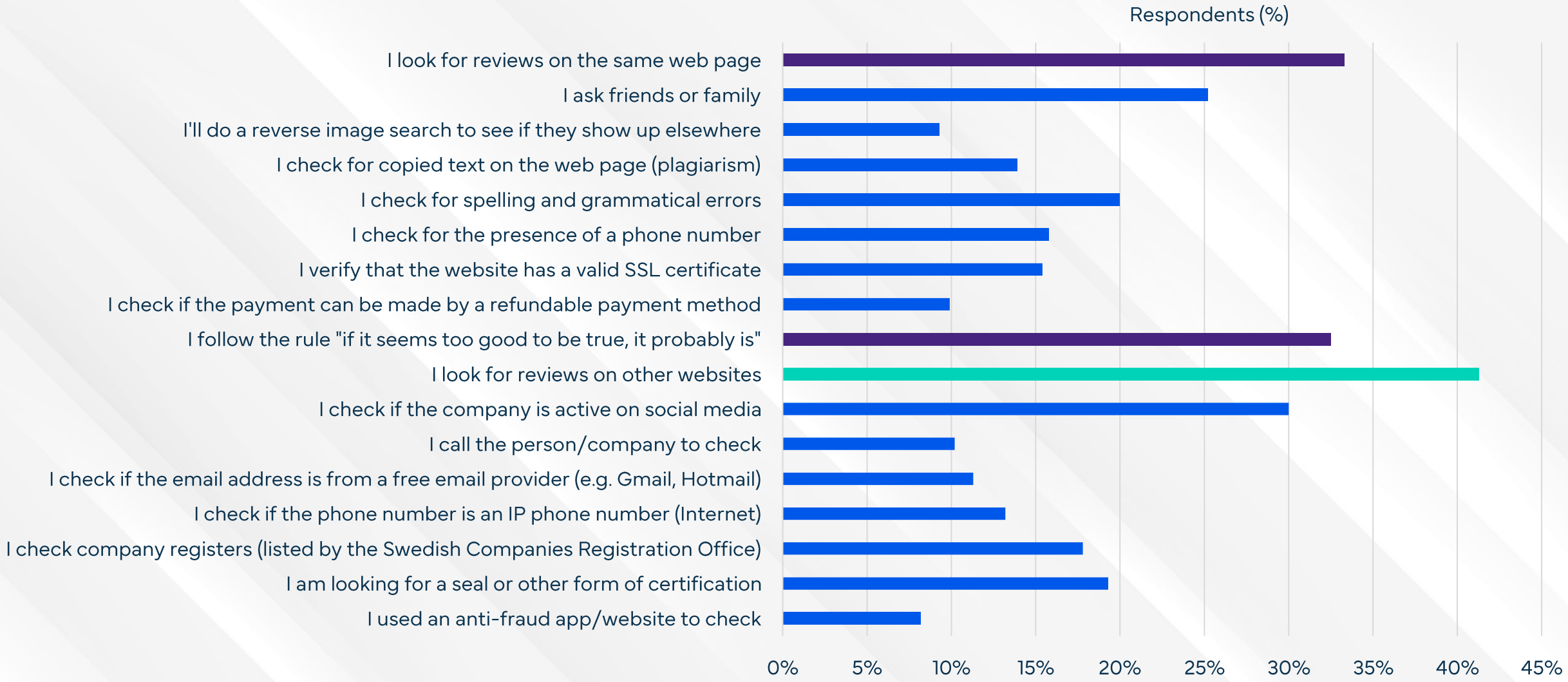


"My friend was scammed by someone pretending to be me and (soliciting) money"

Several victims also reported uncertainty it's a scam but chose to risk it & lacking knowledge to see it.

Q19 - What was the main reason you were deceived?

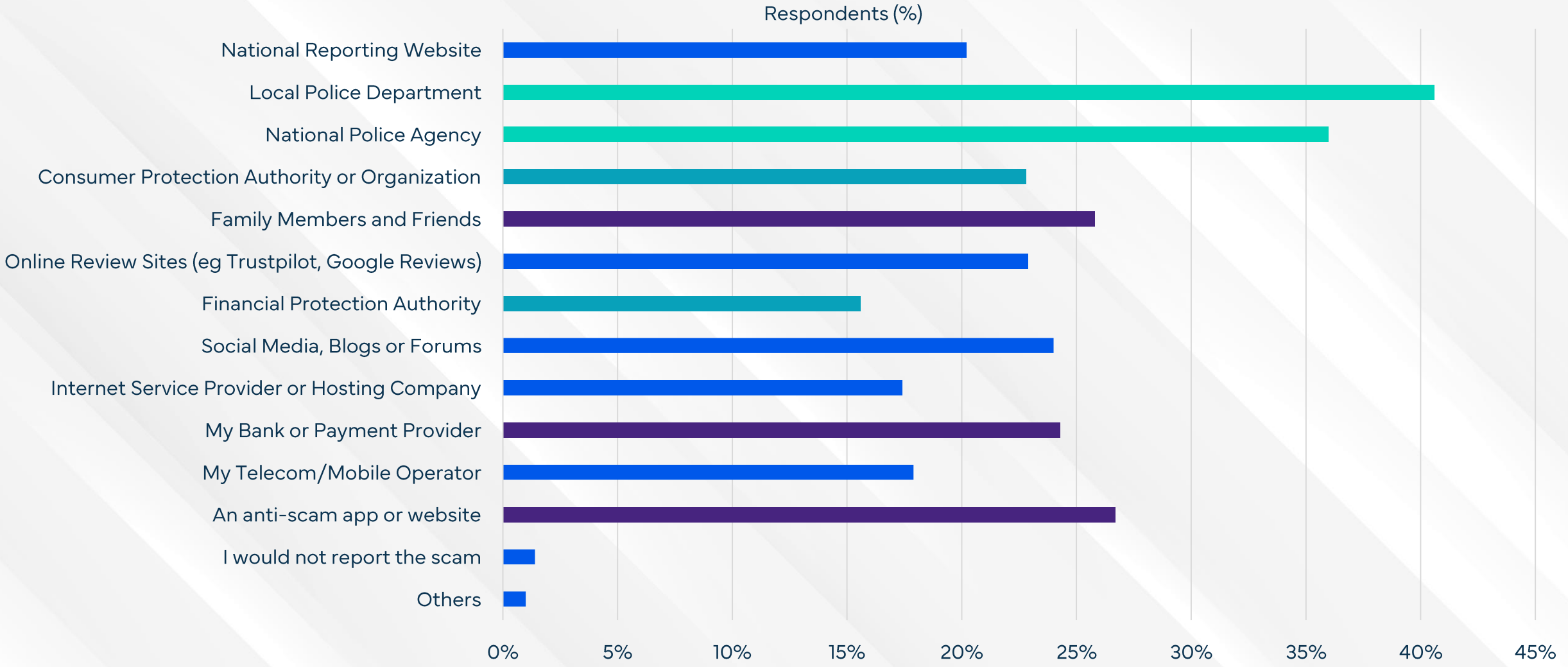
A large proportion of Filipinos check for reviews on other websites



Many reported checking reviews on the same website & following “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?

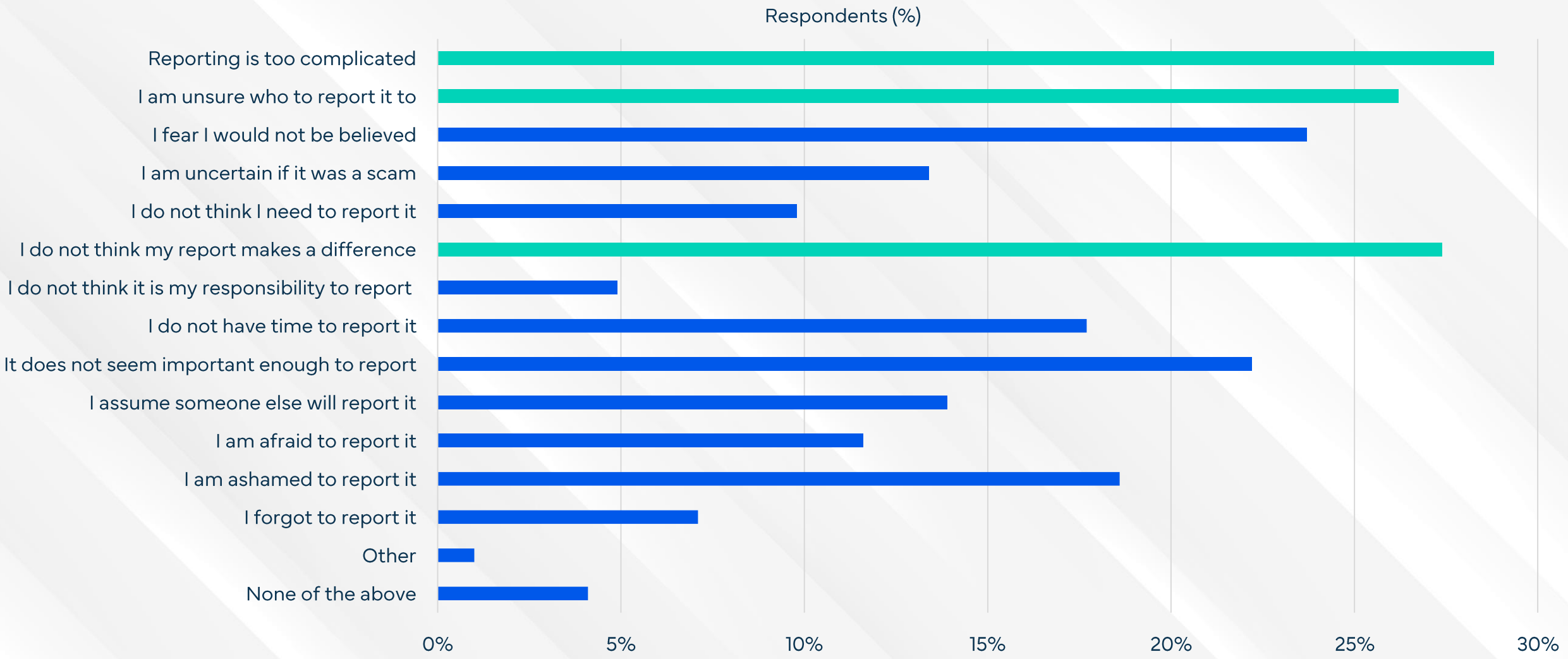
The Police are the favored scam reporting destination



Anti-scam app or websites, family/friends, & banks are also popular places to report scams.

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

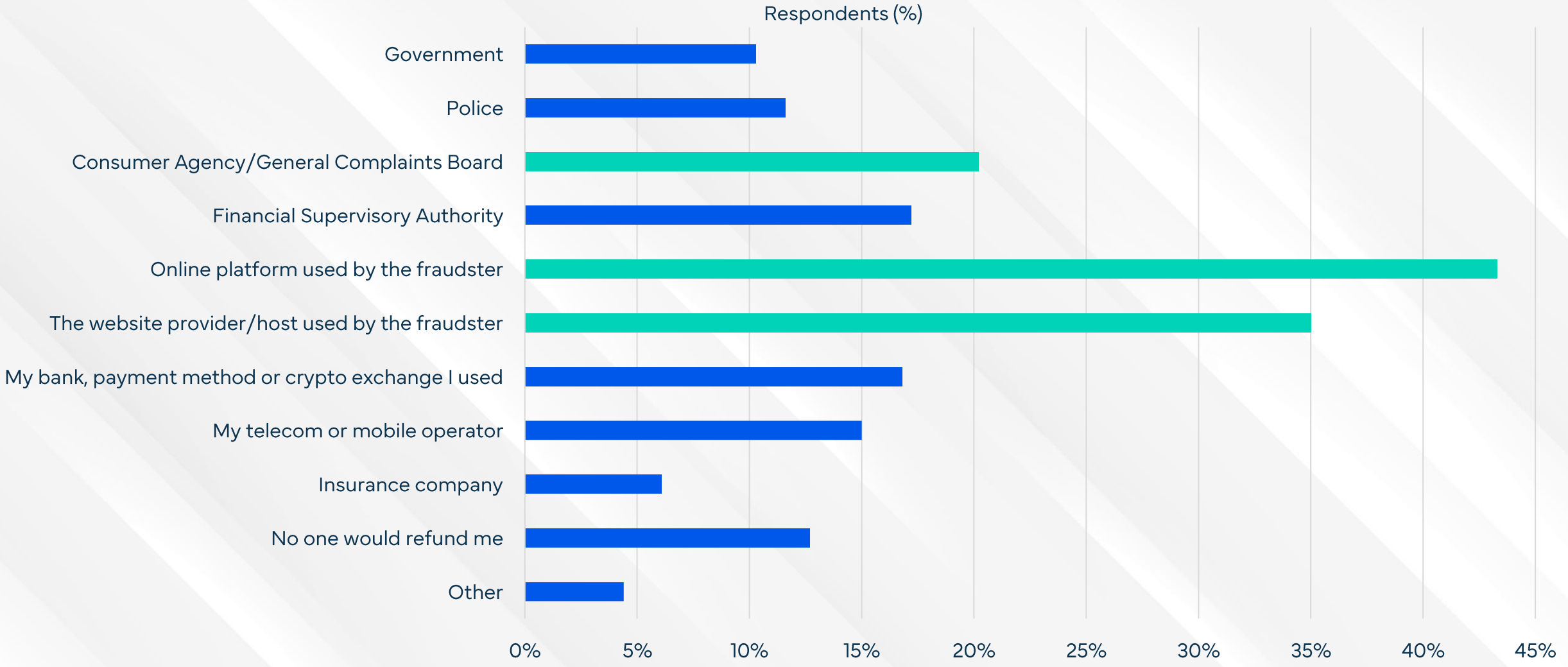
Many Filipinos don't report scams citing complex reporting processes



Other reasons are assuming reporting won't make a difference & uncertainty where to report scams.

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

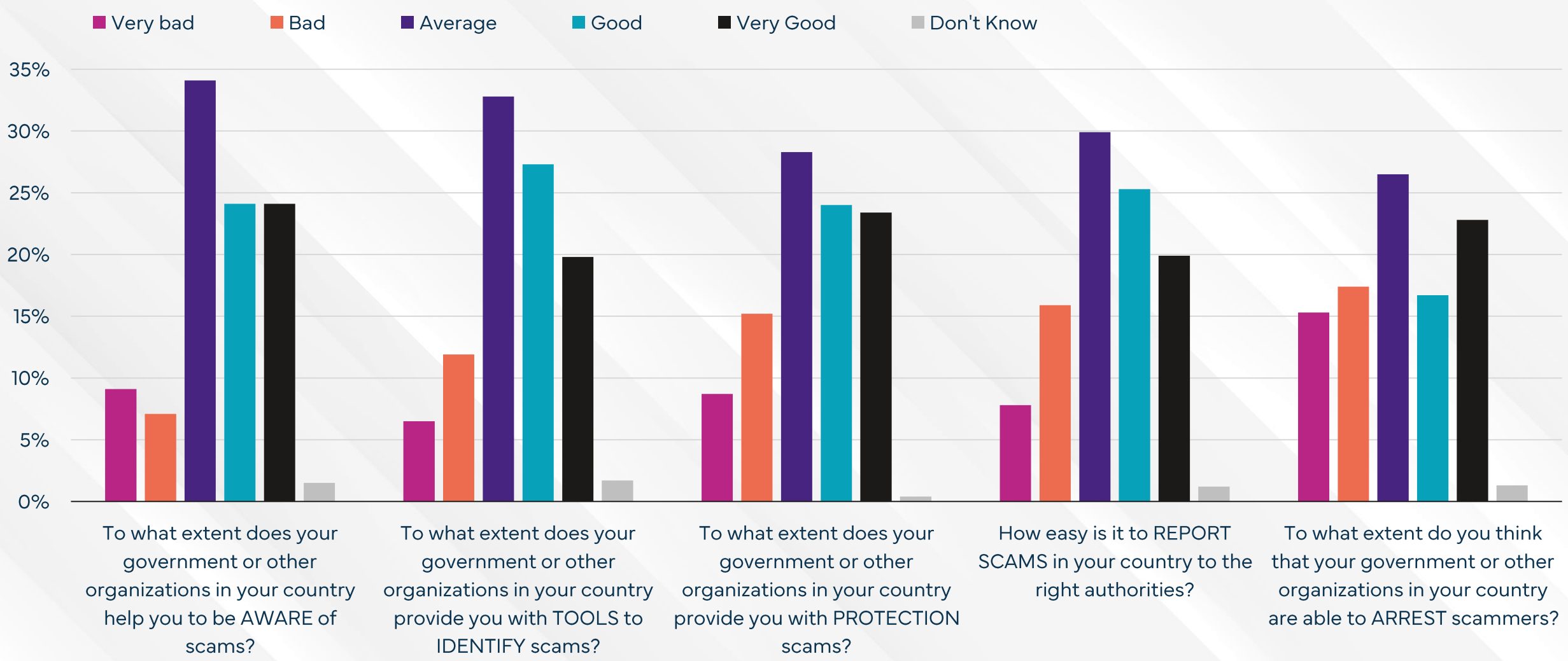
13% of Filipinos assume no one will refund their scam losses



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

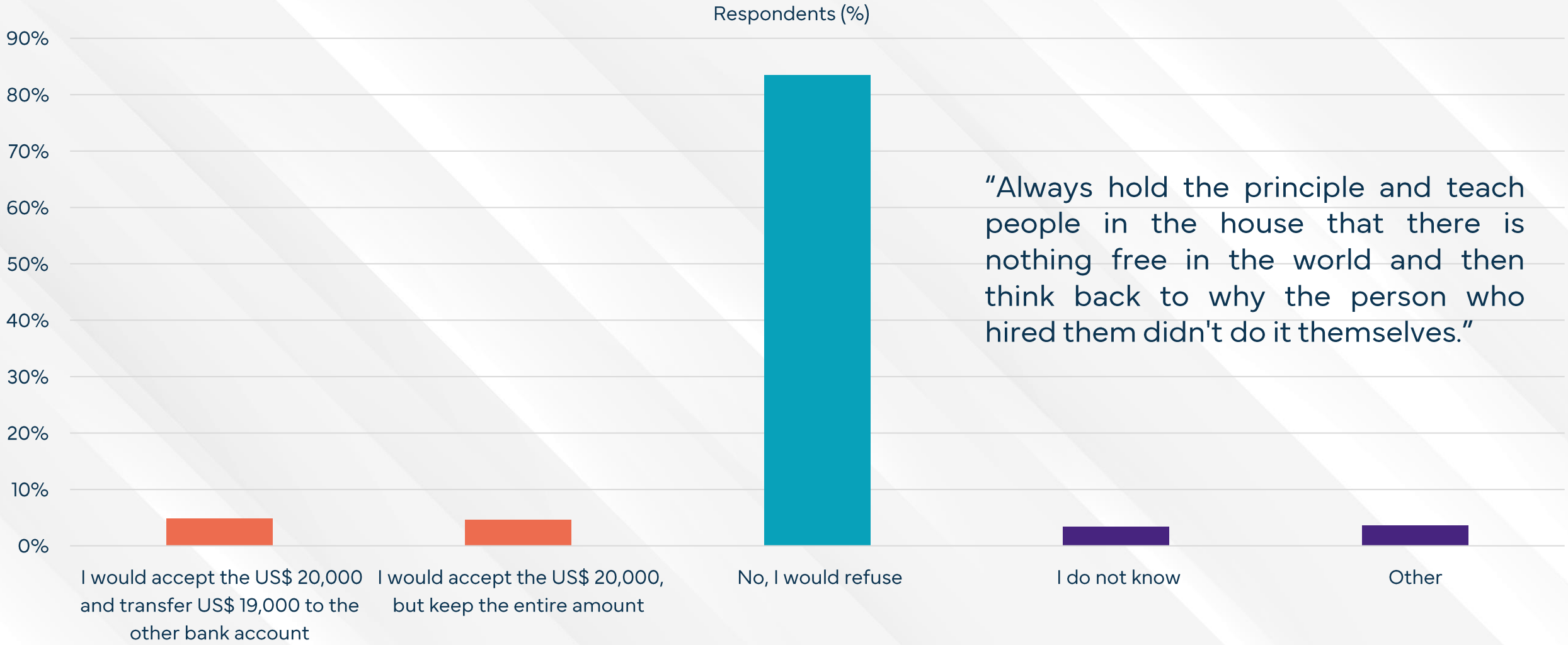
Citizens are unhappy with the Philippines's attempts to arrest scammers



Overall, 23% of the participants rate the actions of the government as poor, 45% as sufficient.

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?

5% of Filipinos admit that they would consider being a money mule



"Always hold the principle and teach people in the house that there is nothing free in the world and then think back to why the person who hired them didn't do it themselves."

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

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.

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.

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.

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

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

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