feedzai

# Global State of Scams Report 2024

GASA
Global Anti-Scam Alliance

# Very little has changed in the last 12 months, as the world's consumers bear the weight of another US$1.03 trillion stolen by scammers

The 2024 Global State of Scams report, conducted by the Global Anti-Scam Alliance (GASA) in partnership with Feedzai, highlights the alarming global rise of scams and the increasing complexity of fraud tactics. Drawing insights from 58,329 respondents across the world, this report sheds light on the state of scams in different regions and the emerging trends shaping the fraud landscape.

Despite global awareness efforts, 67% of people feel confident in their ability to recognize scams, while 9% still lack confidence in their scam detection abilities. China leads in scam recognition with 84% of respondents expressing confidence, followed by Australia at 72%. However, countries like Japan lag significantly behind, indicating a need for better public education.

Scams remain a daily threat for many, with almost half of the world encountering scams at least once a week. In countries like Brazil, Hong Kong, and South Korea, daily scam experiences are all too common. Over the last 12 months, 1 in 2 respondents reported an increase in scam encounters, with Brazil, Australia, and South Africa seeing some of the largest rises. On the other hand, countries like Vietnam, Saudi Arabia, and China reported significant decreases in scam encounters, demonstrating the uneven progress in scam prevention.

Awareness of the use of artificial intelligence (AI) by scammers is growing, but many remain uncertain whether AI was used in their scam encounters. Japanese, Thai, and Malaysian citizens reported the least awareness of AI threats, while globally, 31% of respondents were uncertain whether AI played a role in the scams they encountered.

Phone calls and text/SMS messages remain the primary methods through which scammers operate, with text/SMS scams being particularly common in the Philippines, South Korea, and Brazil. Platforms like WhatsApp, Instagram, and Gmail are also frequently exploited by scammers, with a notable rise in WhatsApp scams across several regions.

Shopping scams remain the most common type of fraud worldwide, with countries like Kenya and Nigeria reporting high rates of online shopping fraud. Conversely, South Korea and Vietnam reported the lowest levels of this type of scam. Investment scams were most prevalent in Nigeria, while identity theft remained a significant concern in Australia and Mexico, each reporting 25% of respondents falling victim to this scam.

The financial toll of scams is staggering, with an estimated $1.03 trillion lost globally in the last year. The hardest-hit individuals were in the U.S., where the average loss per victim reached $3,520, followed closely by Denmark and Switzerland. Developing nations, however, face a more profound impact, with countries like Pakistan losing 4.2% of their GDP to scams, and Kenya and South Africa losing 3.6% and 3.4%, respectively.

Despite these heavy losses, only 4% of global scam victims were able to fully recover their money. Countries like the U.S. and U.K. had the highest recovery rates, but a large majority of victims worldwide were unable to recover any funds at all. This highlights the critical need for stronger consumer protection mechanisms and more effective financial recovery processes.

Emotionally, the impact of scams is severe, with many victims reporting feelings of vulnerability, fear, and a loss of trust. In countries like Kenya, the Philippines, and South Africa, victims experienced the heaviest emotional burdens. Meanwhile, citizens from Japan and South Korea reported feeling the least emotionally affected by scams.

The internet itself is not losing trust worldwide due to scams, though this varies by region. Filipinos and Kenyans reported the greatest decline in trust in the internet, while countries like South Korea and Japan remained largely unaffected in terms of online trust.

In conclusion, the global rise of scams continues to affect millions of individuals, with both developed and developing nations facing unique challenges. While confidence in scam detection is improving, the financial and emotional toll of scams remains high. Global cooperation, improved public awareness, and strengthened recovery processes are essential to combat a growing threat of scams & restore public trust.


Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

# Silver Linings in the Fight Against Scams

The latest GASA report reveals consumers worldwide lost over US$1 trillion to scams in the past year. This is a stunning figure that rivals the GDP of some countries.

But if there's some positive news in these findings, it's this: many vital figures have held steady since last year. The overall share of global respondents experiencing monthly scams remains largely unchanged. It is not just the number of scams that is consistent; losses from scam threats also remained stable compared to the past year. While the scam threat remains severe, the report offers glimmers of hope that efforts to protect consumers are showing progress.

Consumers are also becoming smarter at catching scams themselves. This year, 67% of respondents expressed confidence they could spot a scam. This strong display of confidence is a testament to banks' and others' efforts to educate consumers on the red flags to watch for that could be a scam.

Yet, with over US$1 trillion lost to scams, it's clear that scammers are still succeeding. It's possible that while a significant share of consumers feel confident in their ability to identify a scam, they are still vulnerable. In other words, consumers' confidence in their ability to spot a scam may be making them complacent.

Clearly, there is still work to do to better protect consumers. Given the progress we're seeing, now is the time to step up fraud prevention efforts.

Banks and financial institutions are taking this step by collaborating both inside and outside the financial services industry. This positive news from GASA's findings should further encourage banks—as well as telecom firms, social media platforms, and email providers—to better band together to protect consumers against scams.

One of the most effective ways to protect customers from scams is to understand who they are and how they typically engage with their bank. This knowledge is a decisive advantage that banks and financial institutions have over criminals.

Advanced technology, including AI and machine learning, are critical to understanding if a customer is acting unusually. Having this insight and the ability to respond in real time is essential to stopping scams before criminals can profit.

In their efforts to protect customers, banks are also implementing measures to protect their customers' data privacy concerns. Consider asking customers how they would like to share their data. This approach may give customers greater confidence in their bank that the organization will protect their personal information. Additionally, it could give banks additional data types to analyze and detect scam signals.

These data-based insights will become critical as scam definitions become standardized. Different regions have different ways of referring to scams. For example, the Federal Reserve's Scam Classifier framework in the United States emphasizes who approved a transaction and whether urgency or pressure was used to manipulate victims. The European Banking Authority, meanwhile, offers a common fraud taxonomy for European banks to report different types of fraud and scams. Other countries have their own classification schemes. Establishing a standard description of scams is essential in understanding how scammers operate. This is the critical first step in stopping them.

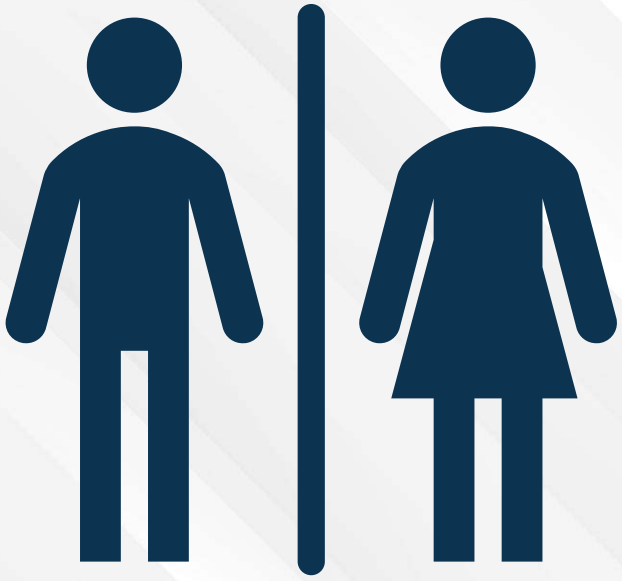
Feedzai's collaboration with GASA underscores our shared commitment to safeguarding bank customers from scams. By leveraging cutting-edge AI and machine learning technology, we're helping financial institutions detect unusual behavior and prevent fraud in real time. But protecting customers goes beyond technology—it's about fostering industry-wide collaboration and ensuring data privacy, so customers feel confident sharing their information. Together with GASA and our partners, we are driving continuous innovation to stay ahead of evolving scam tactics, ensuring a safer financial ecosystem for everyone.

No one can afford to operate in silos, least of all banks. We must all continue to collaborate across the industry and pull in third-party data whenever possible to clearly understand a customer's risk of being scammed.

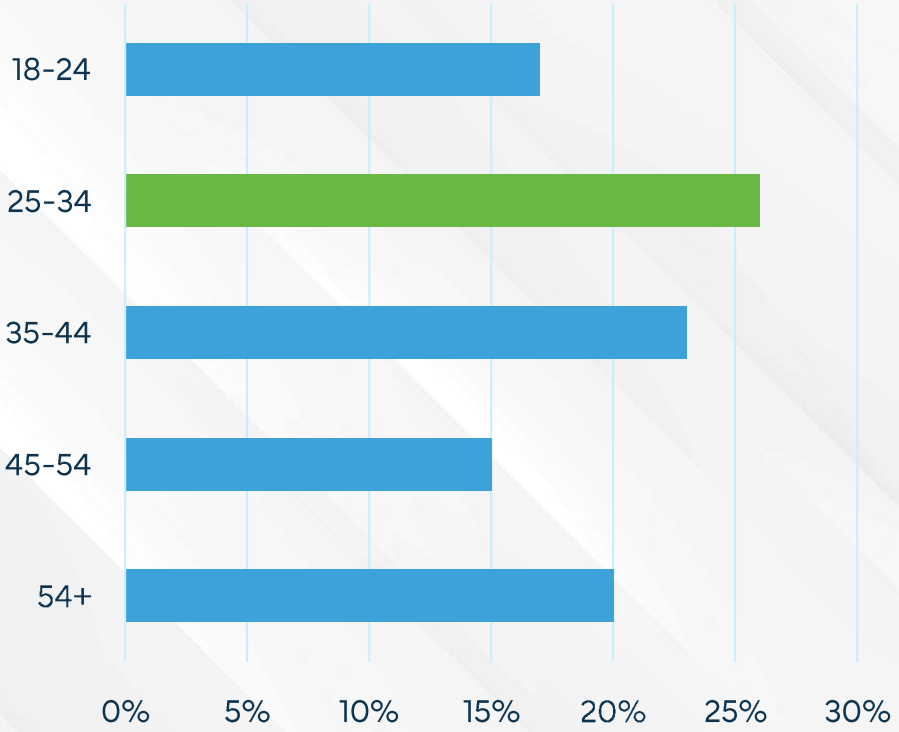
Nuno Sebastião
Co-Founder, Chairman, and CEO
Feedzai

# 58,329 people participated in the Global State of Scams survey

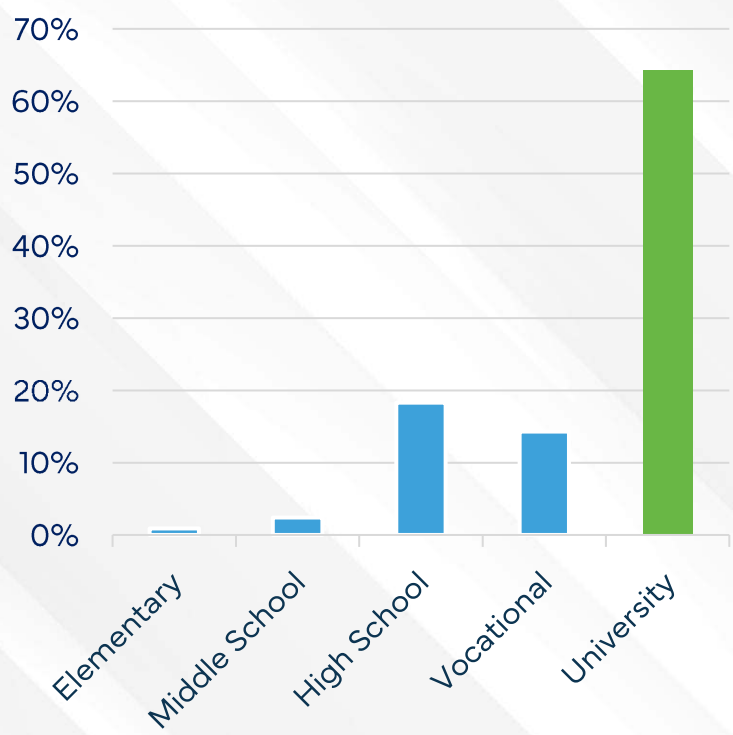
## Gender




## Age Range

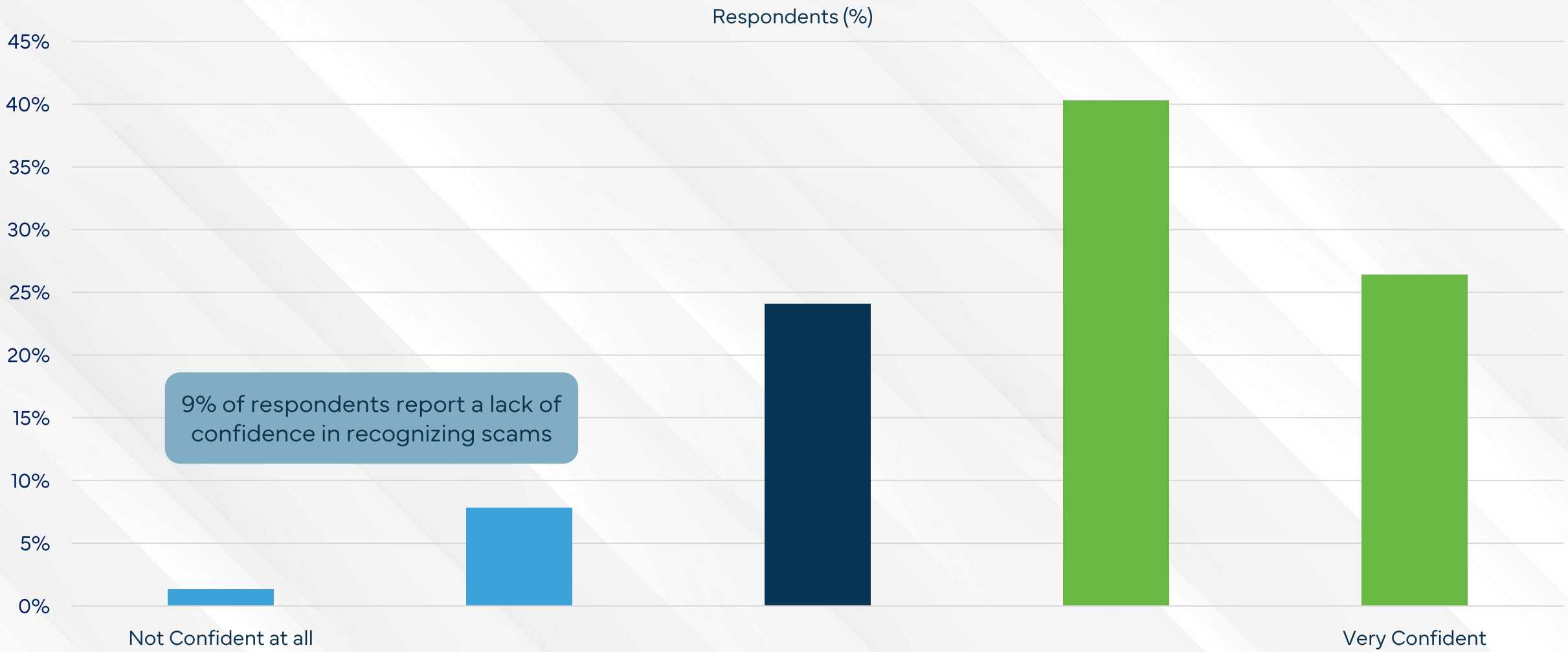



## Education




The demography of survey respondents varied by country. Overall, we approached slightly more males than females, with over a quarter of respondents falling into the 25–34 age group. The vast majority were educated to a university or postgraduate level.

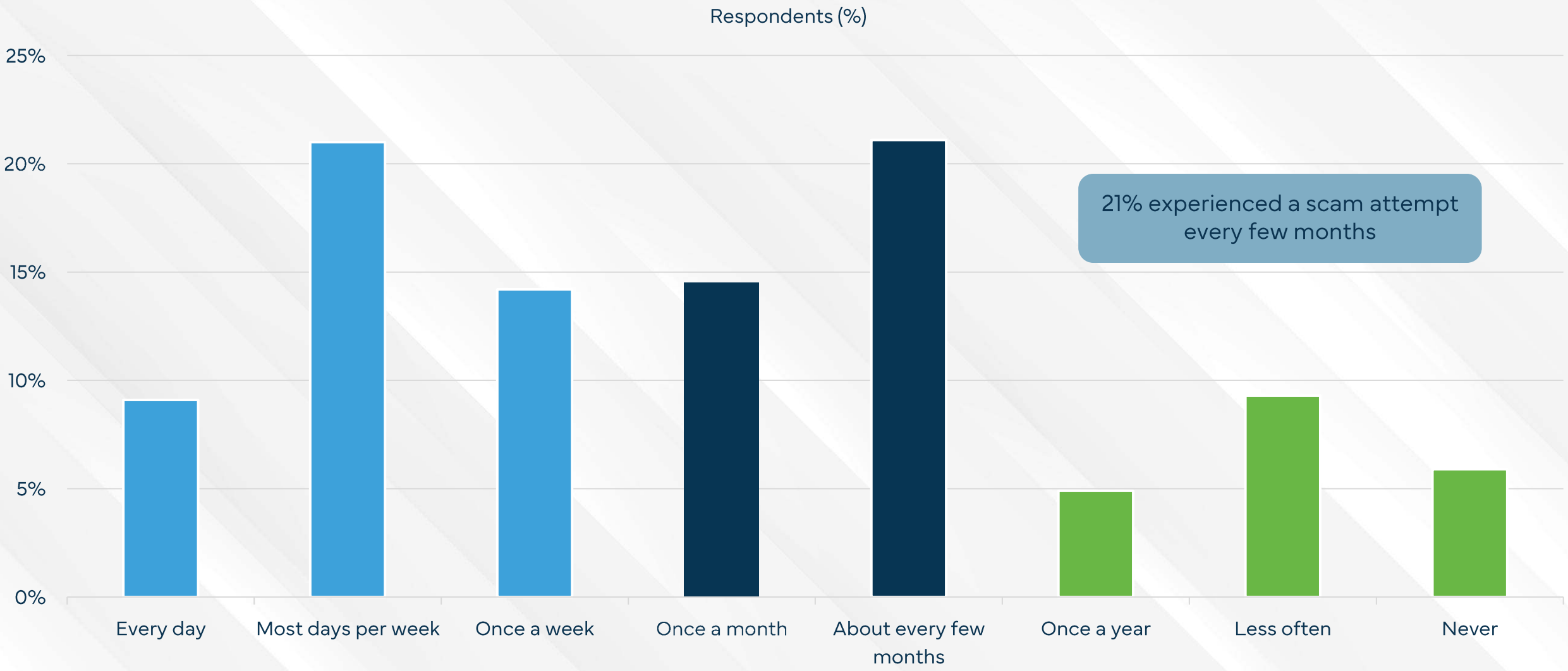
# 67% of world citizens believe they have the skills to recognize scams




China (84%) & Australia (72%) are most confident in their scam detection abilities, while confidence lacks severely in Japan (38%).

How confident are you that you can recognize scams?

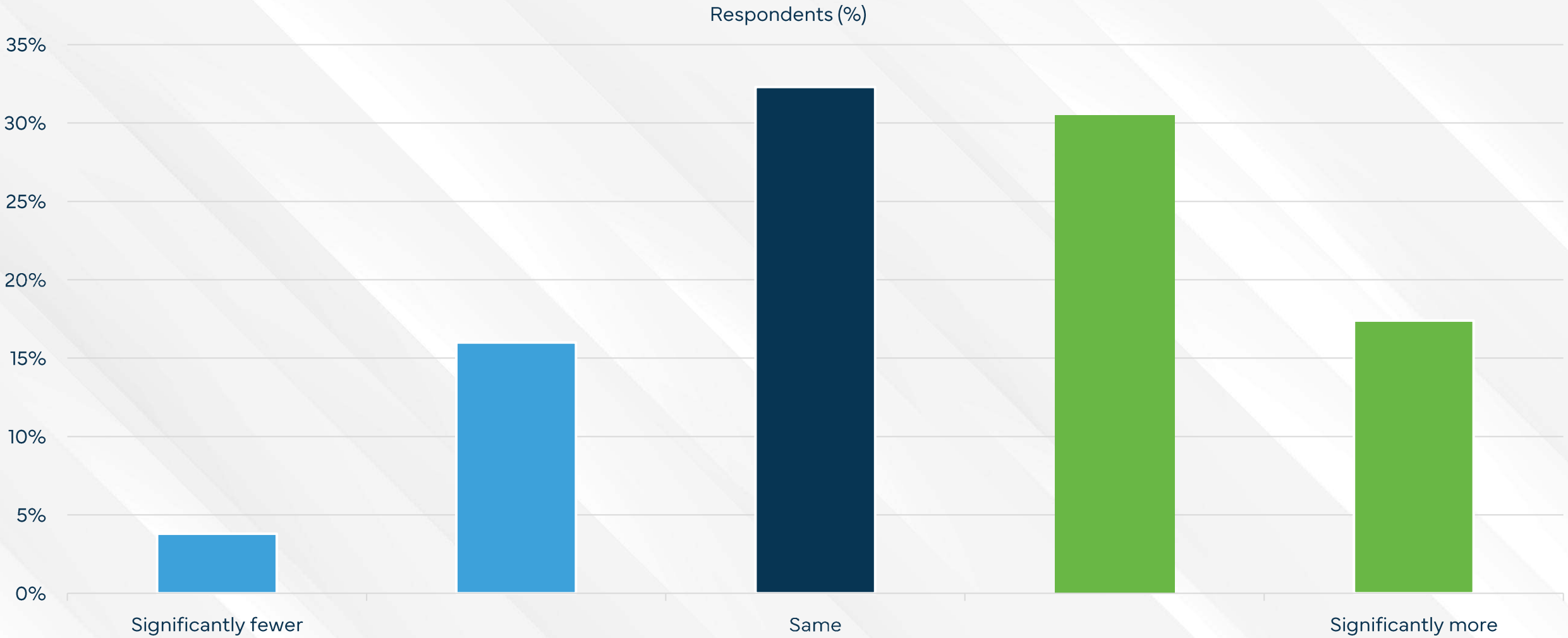
# Almost half of the world encounter a scam at least once a week




41% of Brazilians encounter scams every day, Hong Kong (33%) and South Korea (26%) citizens also report daily scam experiences.

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.

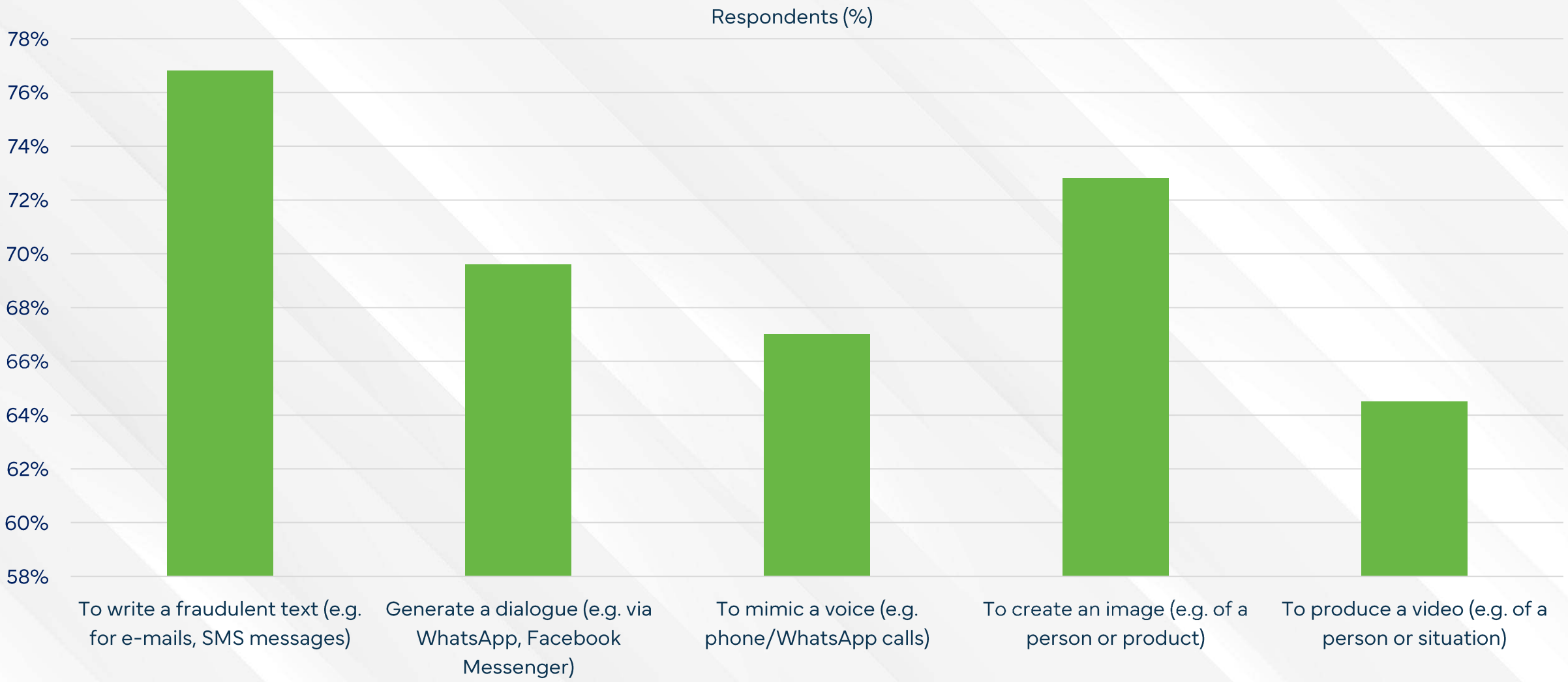
# 1-in-2 respondents were exposed to more scams in the last 12 months




Globally, 1-in-5 experienced fewer scams than the previous year. Brazil (63%), Australia (64%), and South Africa (58%) report an increase in scam encounters, while Vietnam (45%), Saudi Arabia (37%), and China (35%) all report significant decreases over the last 12 months.

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?

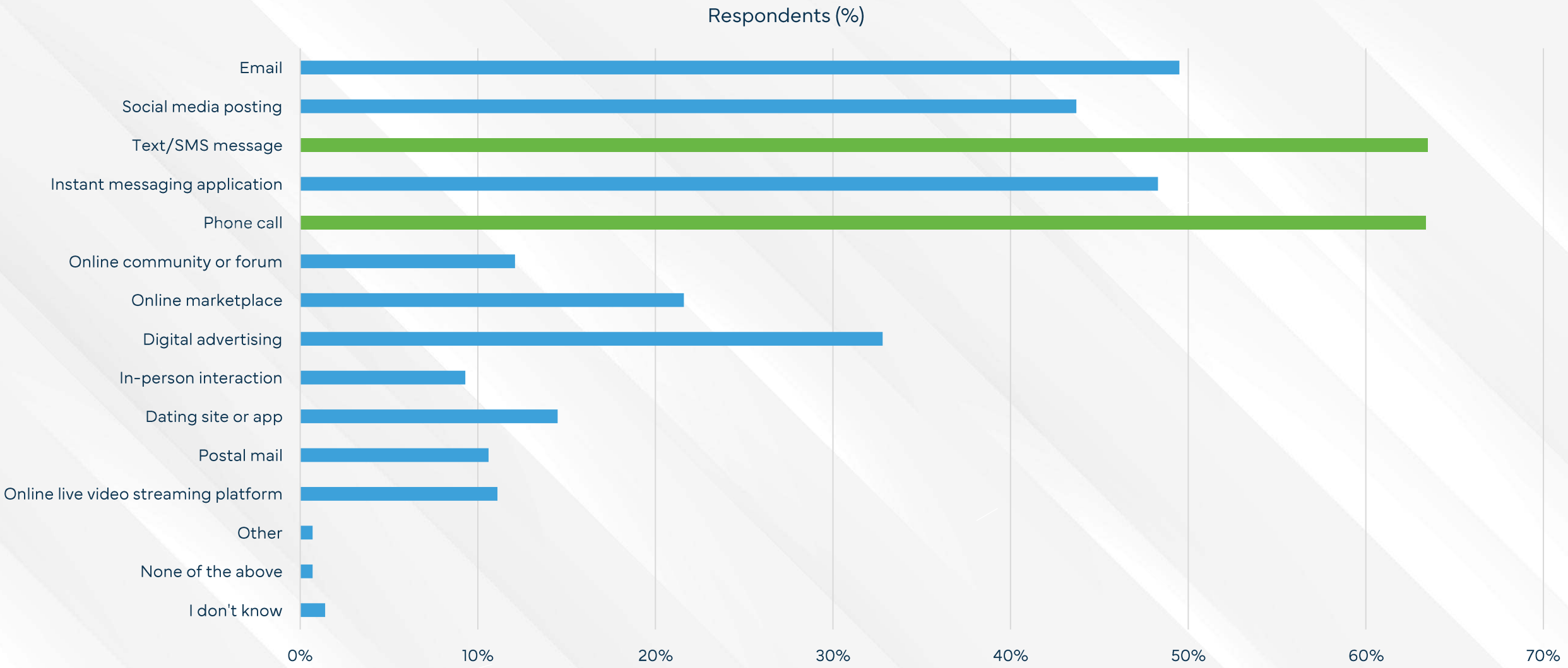
# Overall awareness of AI threat capabilities is increasing worldwide




Japanese (15%), Thai (12%), and Malaysian (11%) citizens admit a lack of knowledge of AI threat capabilities of scammers.

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

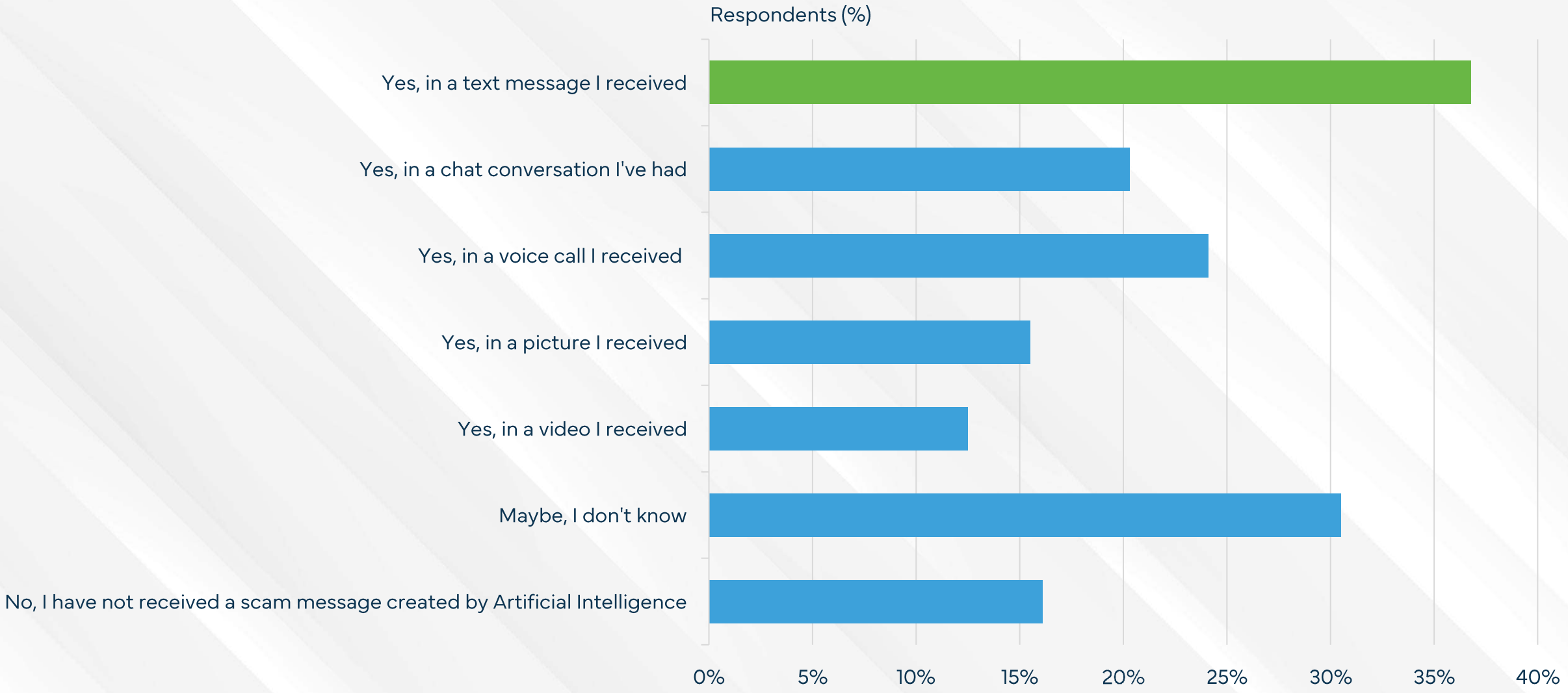
# Phone call scams are most common in Thailand, Russia & Hong Kong




Text/SMS Messages are the common scam delivery method in the Philippines (86%), South Korea (85%), Kenya (84%) & Brazil (82%).

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

# Globally, 31% are uncertain whether AI was used to scam them




## 16% do not believe AI was used against them by scammers.

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

# The stories of scam victims from around the world

feedzai GASA Global Anti-Scam Alliance

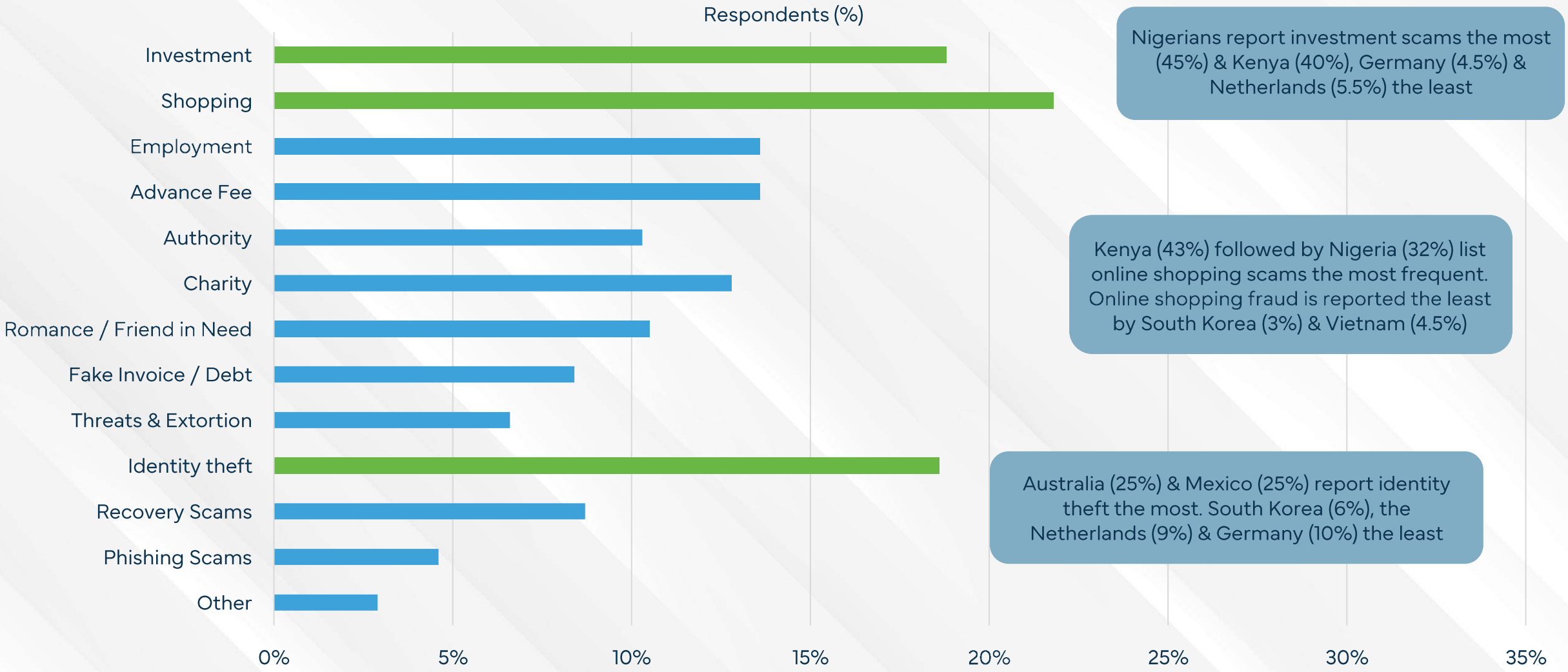
"I paid £20 for an item for my child's birthday but it turned out that what I had paid was a subscription where I would never receive the item, and they would take money from my account every month." – **United Kingdom**

"Someone sent me an SMS claiming to have sent important and delicate ship cargo information by mistake and asked me not show the details to anyone else. He went ahead to claim that I could go to the port to clear the cargo for him at a fee since he was outside the country, and since now I was in the know of the particular details, he requested I send the bank account where he would send me money, but I saw through his lies and declined. " – **Kenya**

"The scammer obtained my Facebook password (No idea how) and accessed my email through messages on messenger. My password was the same. Eventually, the scammer stole close to 1000$ from a casino account where I also used the same password. I now have a different password for EVERYTHING!" – **Canada**

"I was contacted by someone who offered me a work-from-home opportunity with a good salary. Since working from home has always been a dream of mine, I was excited about the prospect and decided to give it a try. I completed a 7-day training program as instructed, but after that, I was asked to pay $70 to start earning. Trustingly, I made the payment, expecting to begin the actual job. Unfortunately, the individual took my money and disappeared, leaving me disappointed and financially disadvantage." – **New Zealand**

# Shopping scams are the most frequently encountered scams in the world




Nigerians report investment scams the most (45%) & Kenya (40%), Germany (4.5%) & Netherlands (5.5%) the least

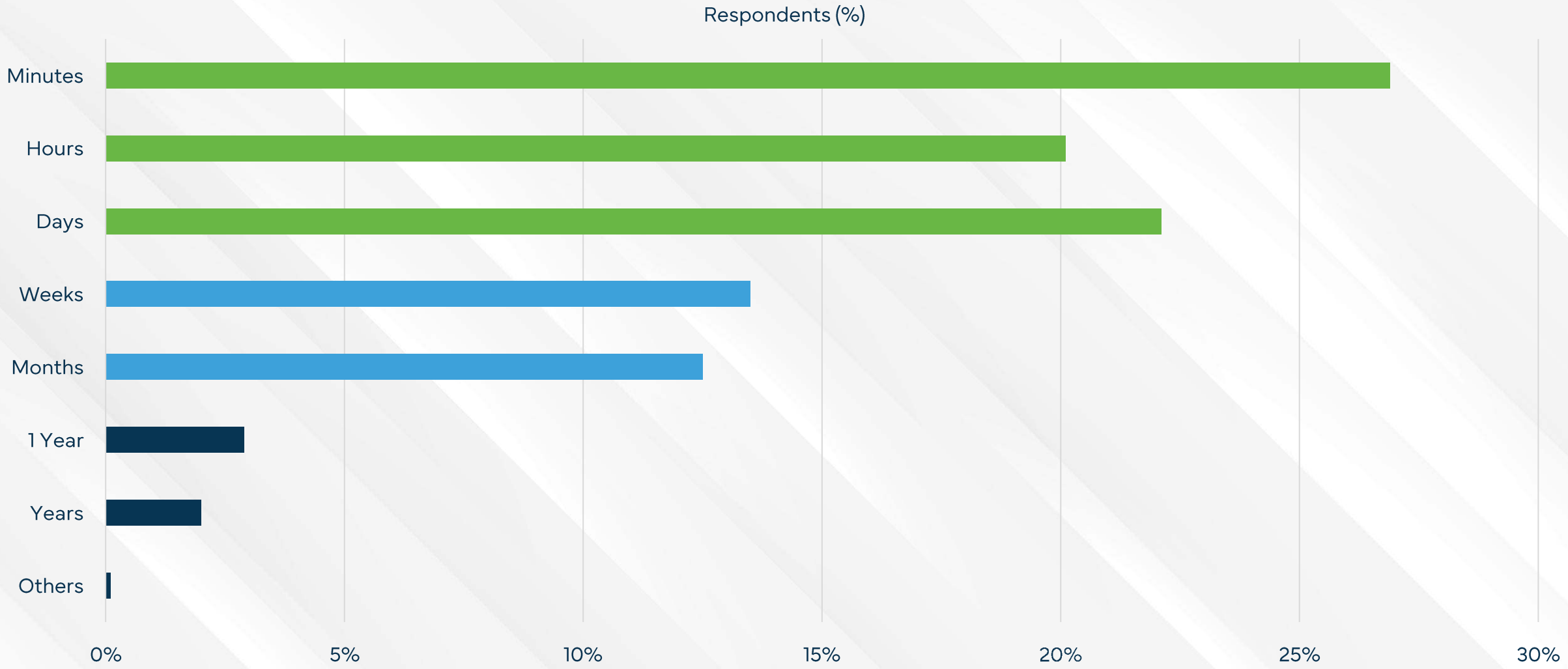
Kenya (43%) followed by Nigeria (32%) list online shopping scams the most frequent. Online shopping fraud is reported the least by South Korea (3%) & Vietnam (4.5%)

Australia (25%) & Mexico (25%) report identity theft the most. South Korea (6%), the Netherlands (9%) & Germany (10%) the least

22% encountered at least one shopping scam, followed by investment fraud (19%) & identity theft (17%).

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

# Nearly half of all scams worldwide are over within 24 hours of the first contact




3% of global scam experiences took place over a year, with 2% sadly facing scams that last years at a time.

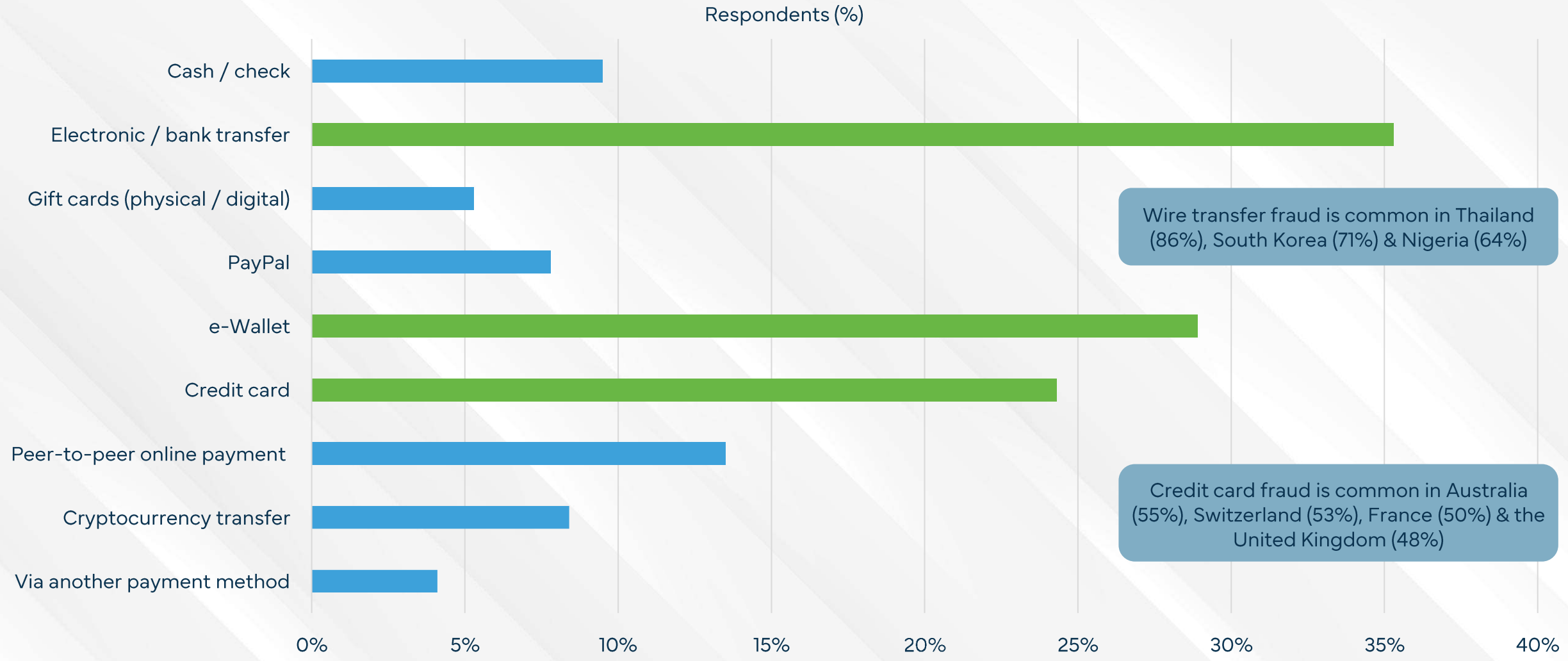
How long did the scam last, from the first time you heard from the scammer until the last payment you made or the last time you contacted them?

# 74% concluded for themselves that they were victim of a scam


22% were notified by friends/family while media/news & banks are also popular in pointing out scams.

Q13 How did you discover you were scammed?

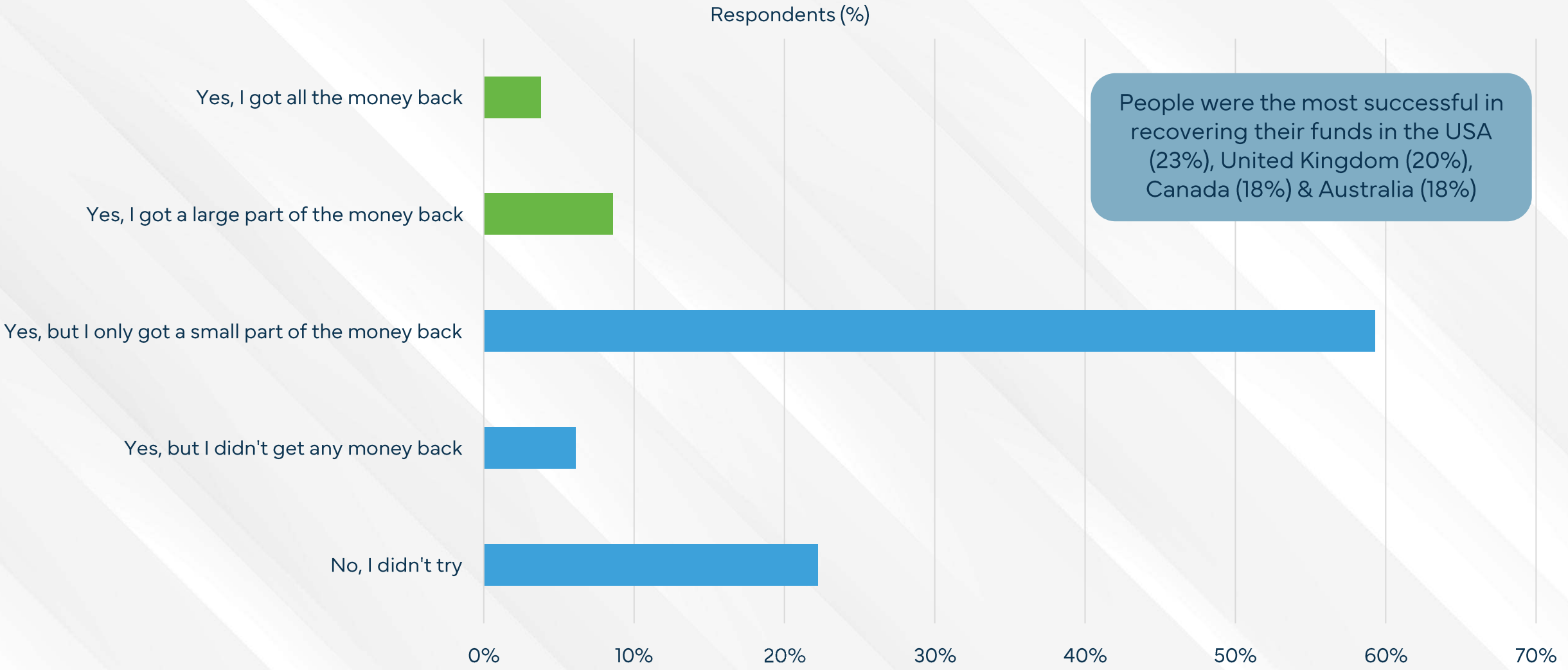
# Bank Transfers & e-Wallet are the dominant scam payment method




Credit cards & peer-to-peer payment are popular, while gift cards are less popular globally.

How did you pay the scammer?

# Globally, only 4% of the participants were able to recover all money lost

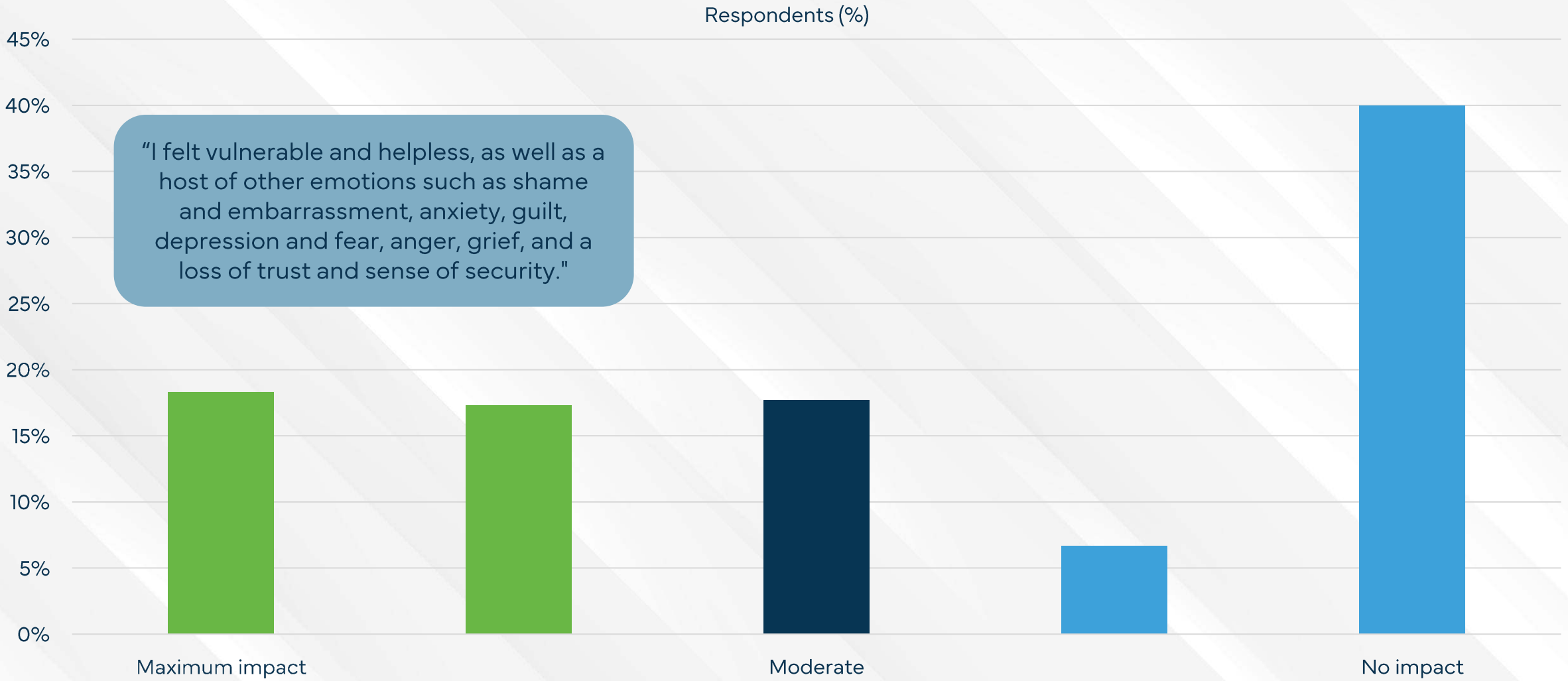



People were the most successful in recovering their funds in the USA (23%), United Kingdom (20%), Canada (18%) & Australia (18%)

22% did not try to recover their funds. 59% tried but were unable to recover any money.

Did you try to recover the money lost?

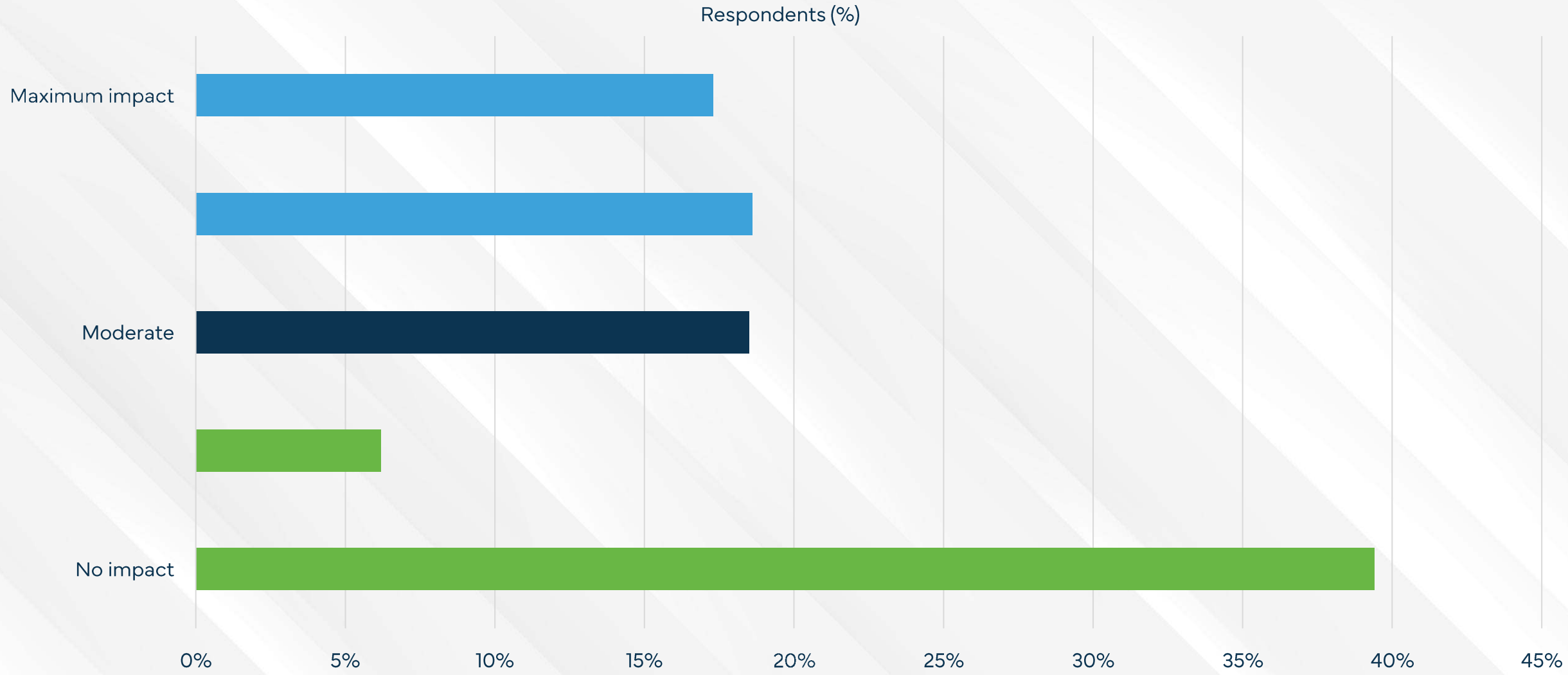
# 36% of scam victims report a severe emotional impact after a scam




Kenyans 61%, Filipinos 57% & South Africans 56.5% reported the most severe emotional impacts due to scams, with Japan 81%, South Korea 81% & the Dutch 77% reporting the least.

To what extent do scams impact your trust in the Internet, in general?

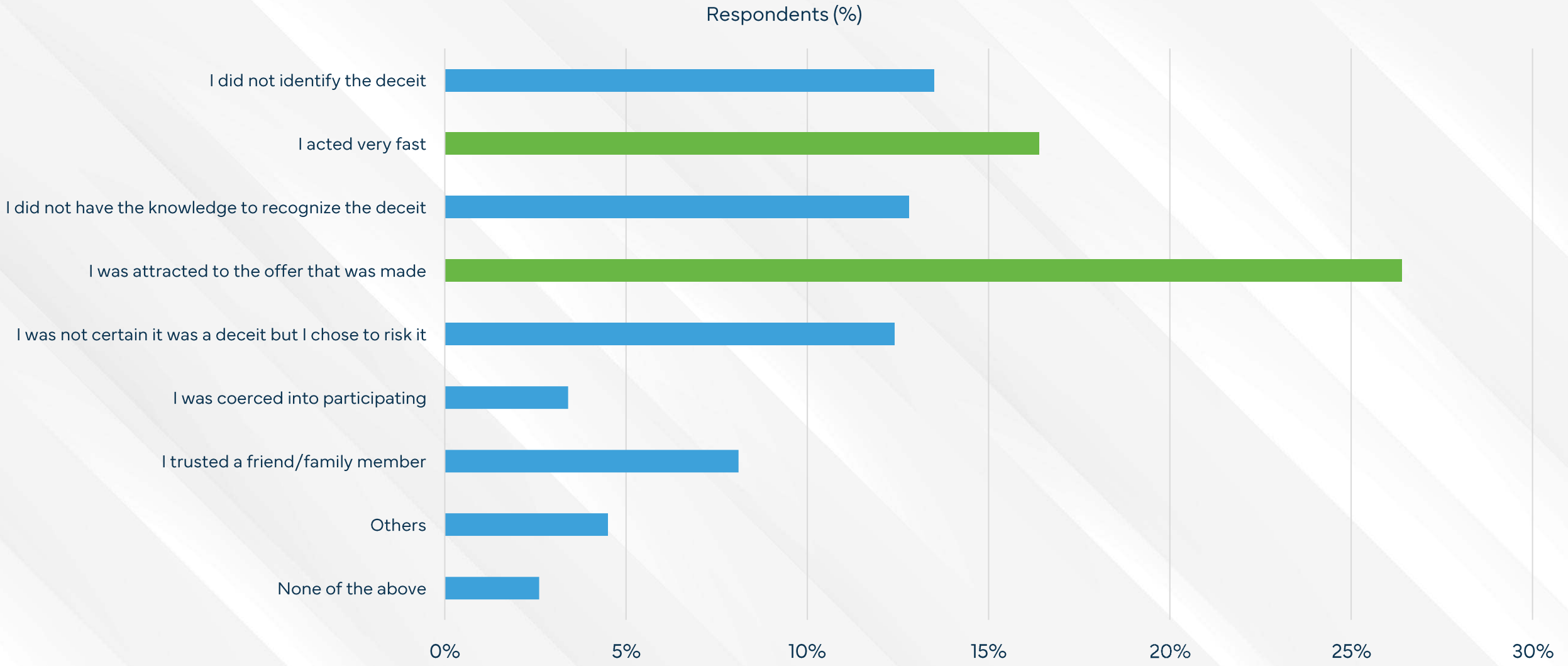
# The impact of scams generally does not degrade trust in the Internet




Filipinos (62%), Kenyans (56%) and South Africans (56%) reported losing the most trust in the internet due to the impact of scams, with South Korea (77%), Japan (74%) and the Netherlands (71%) largely found their level of trust in the internet unaffected.

To what extent do scams impact your trust in the Internet, in general?

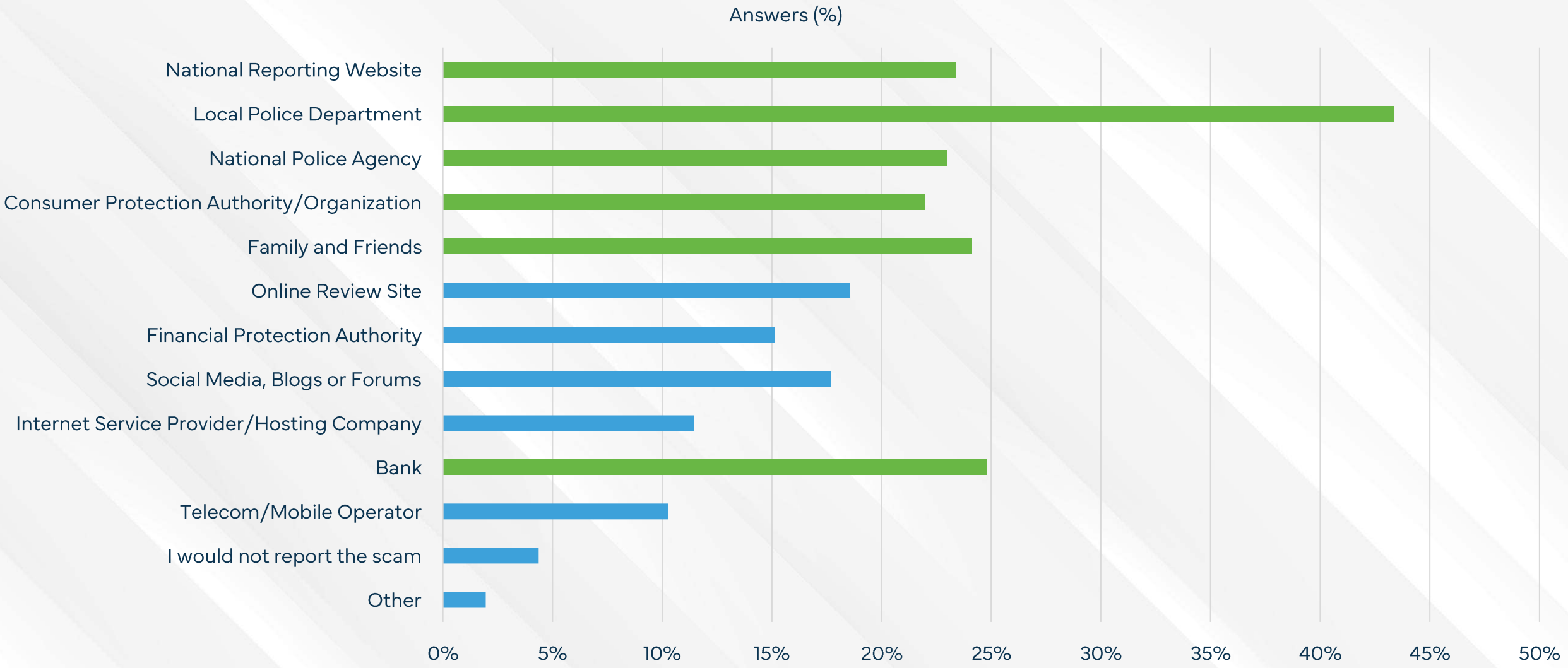
# Many victims are caught out by reacting quickly to attractive offers




A sizable portion of victims simply did not detect the scam or didn't have the knowledge required to spot scams.

What was the main reason you were deceived?

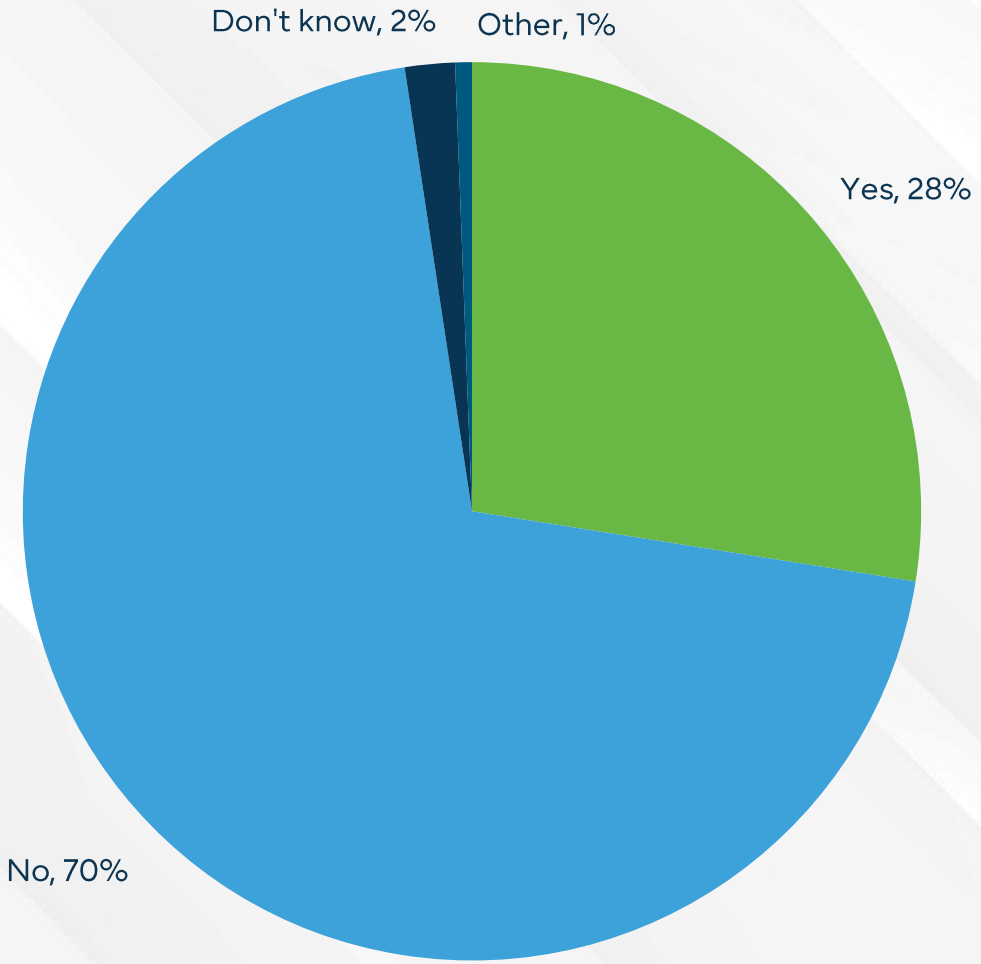
# Most scam victims turn to their local police, while 1-in-4 will report straight to their bank




Hong Kong (59%) & China (54%) turn to National Reporting Websites, 1-in-4 Egyptians do not tell anyone about the scam at all.

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

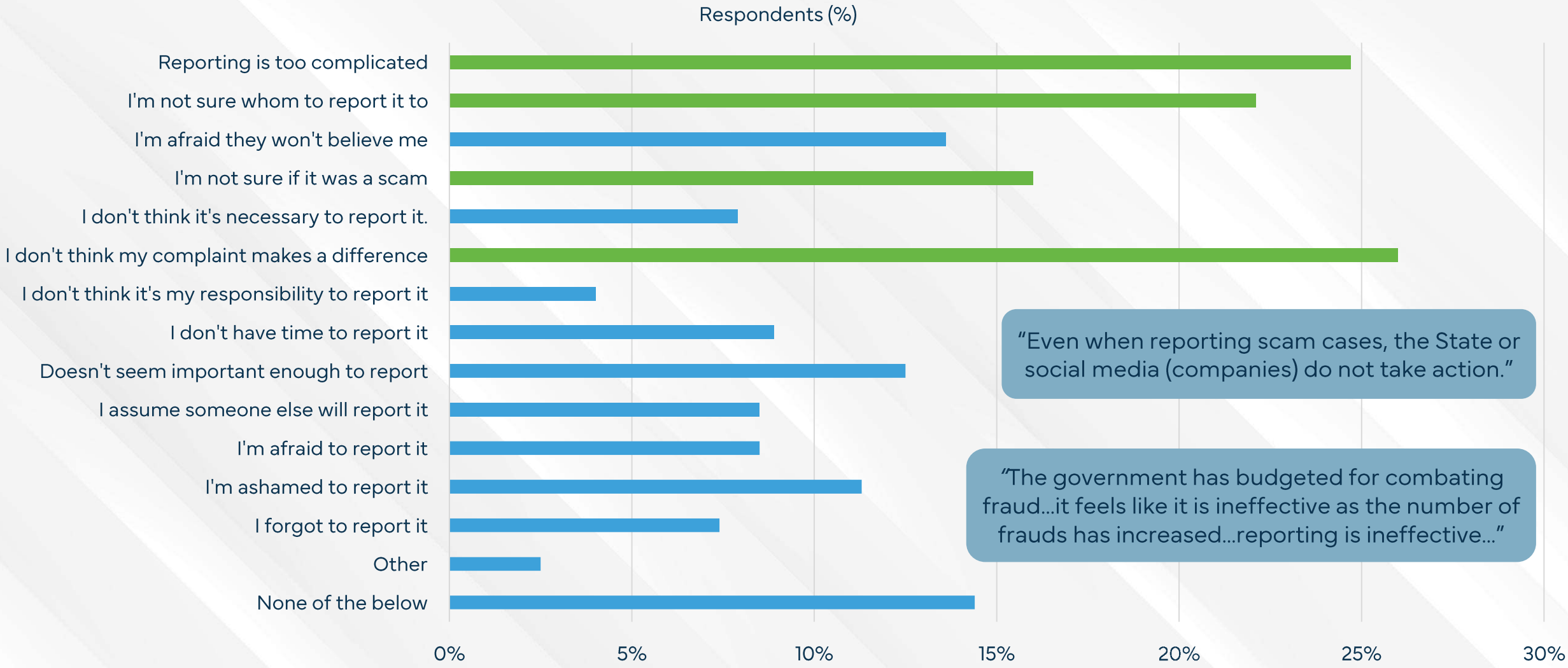
# 70% of people did not report the scam to law enforcement




28% stated having reported the scam to law enforcement or another government authority.

Did you report a scam or scam attempt to the police or authorities in the last 12 months?

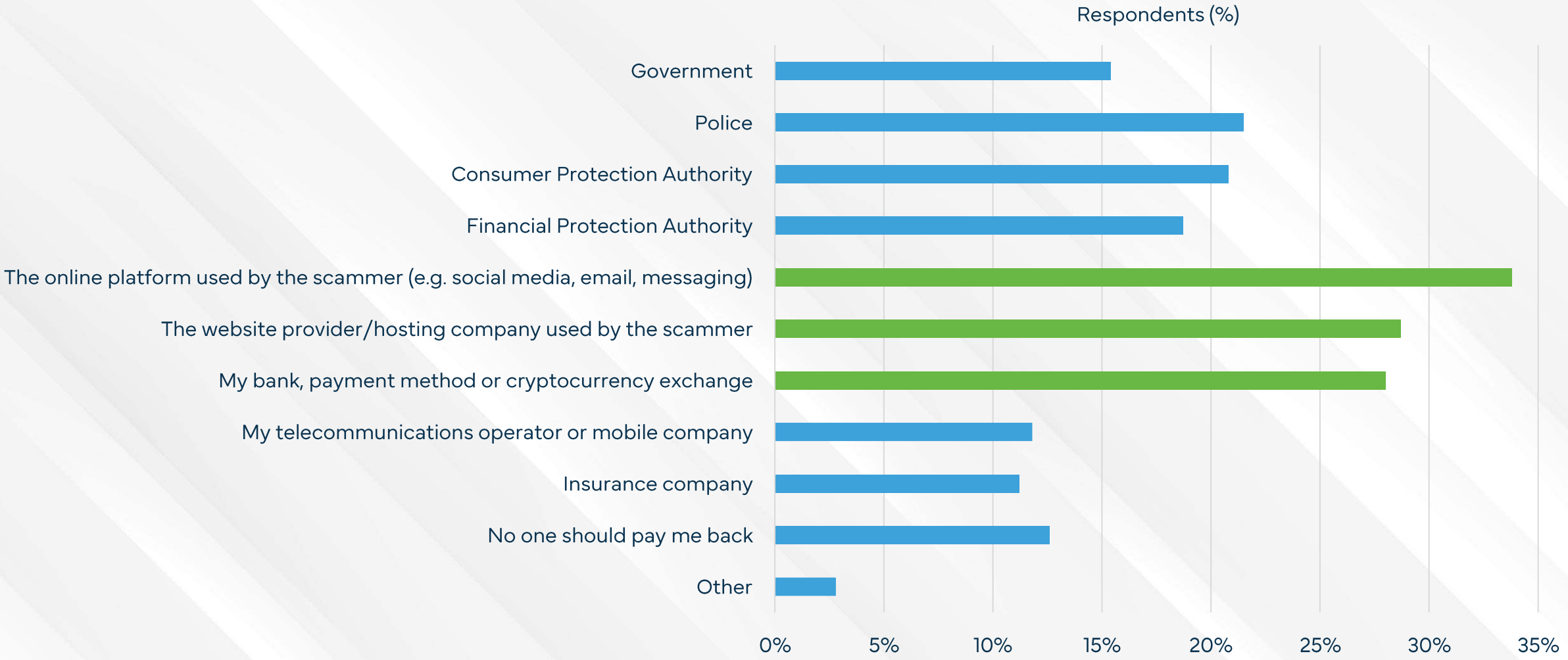
# Many around the world stay silent on scams, with many feeling the the reporting processes are convoluted or an exercise in futility




Some lack clarity on where or to whom they should be reporting, while others question if what they are experiencing is a scam at all.

What reasons might you have to not report a scam?

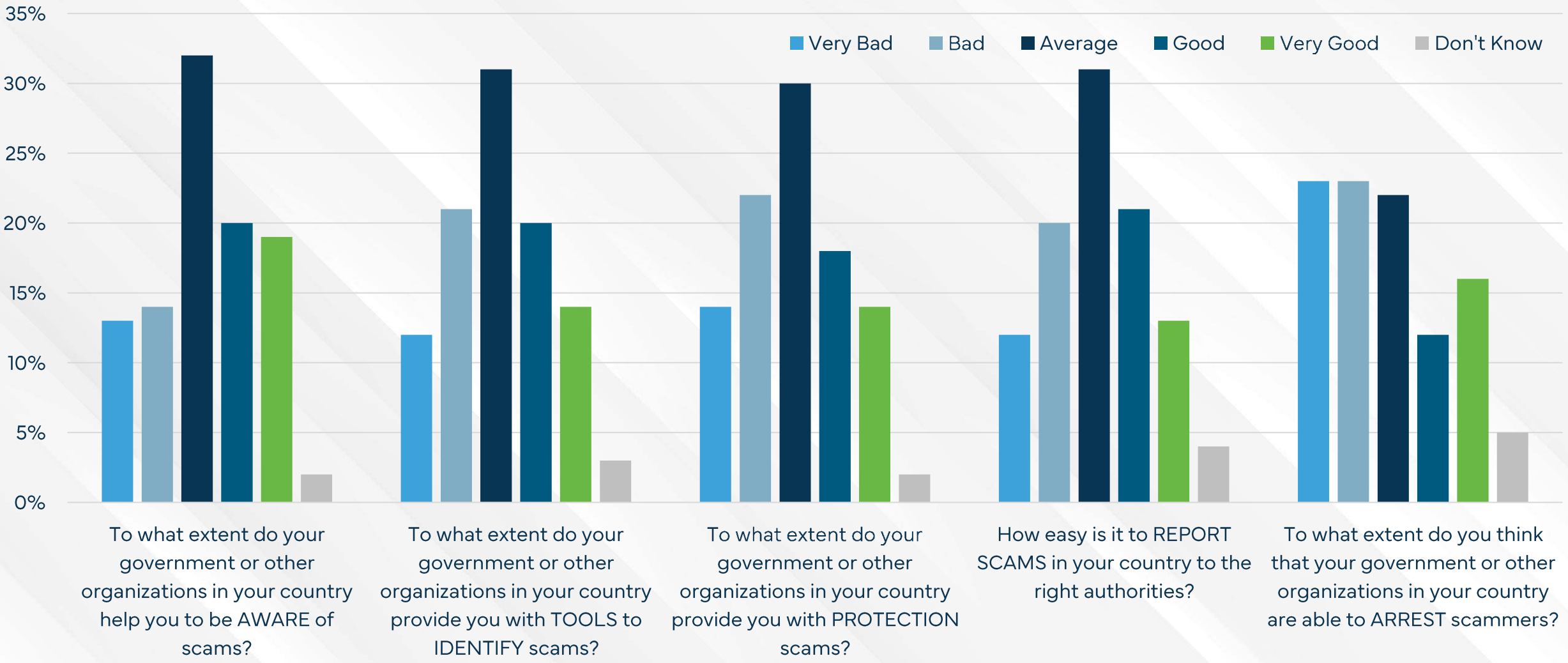
# 1-in-10 globally assume no one will refund scam losses




Many believe the responsibility for refunding victims should lay with the platform scammers use, along with website hosts and banks.

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

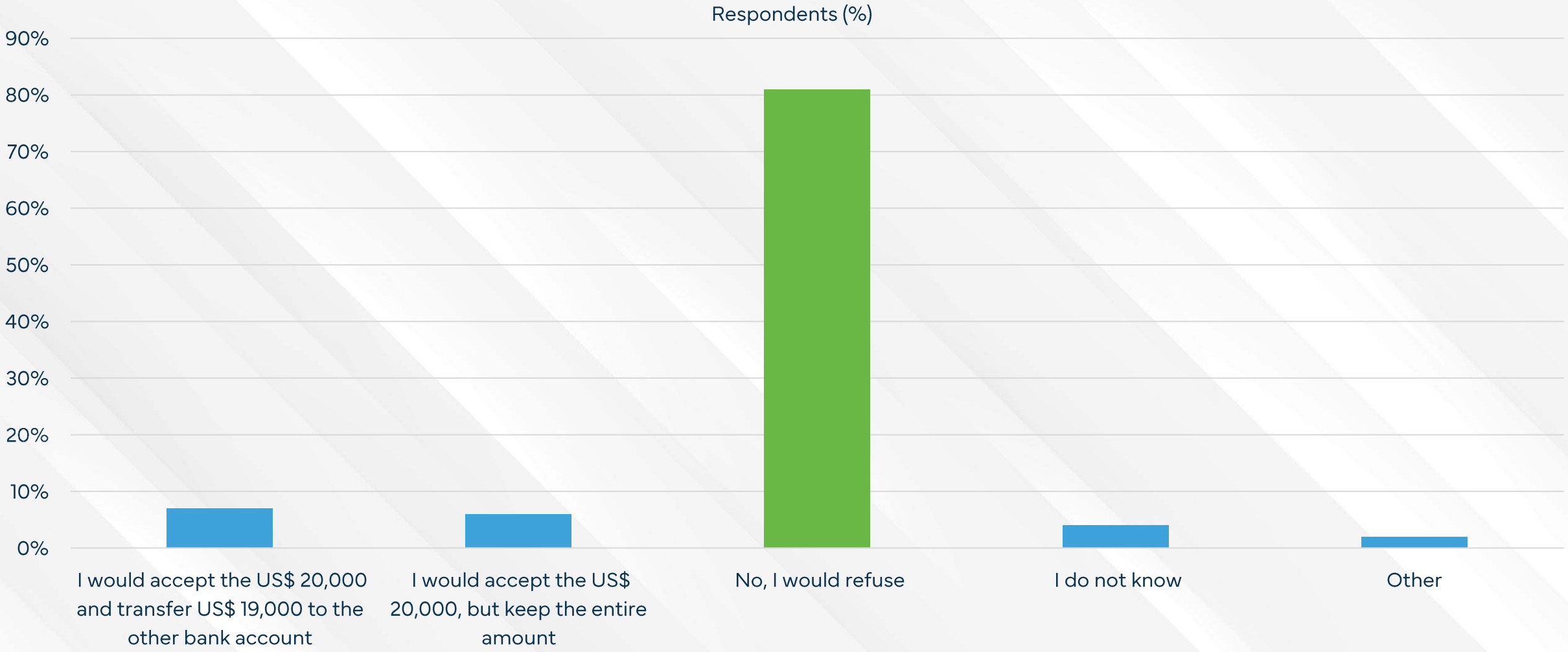
# Frustration mounts globally over the slow pace of scammer arrests




The citizens of the United Arab Emirates ranked as the most satisfied with their government's efforts to arrest scammers, while the Saudi Arabian people believe their government is adept at providing tools for their citizens to identify scams.

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?

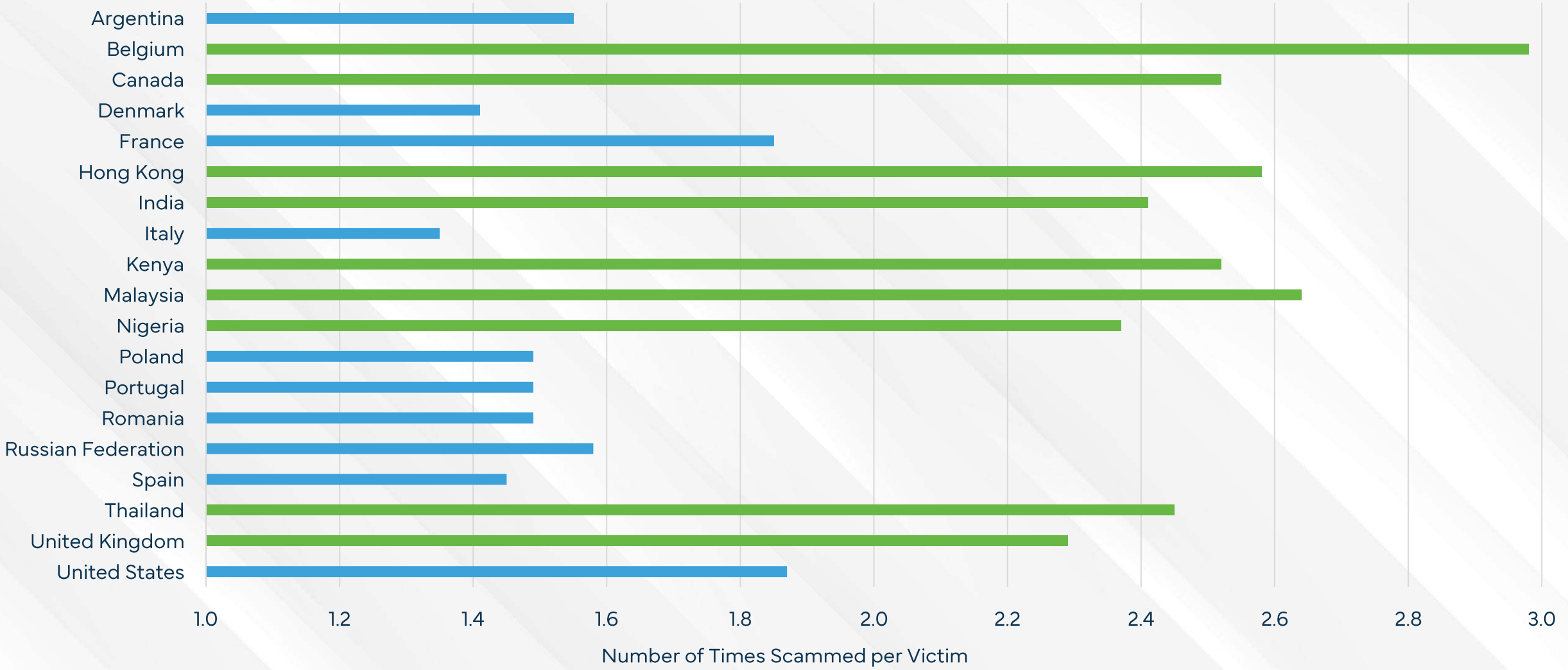
# 7% of people globally admit they would take part in “money muling”




13% would knowingly accept a fraudulent payment into their account, however, 81% of world citizens claim that they would refuse to take part consider taking part in such a fraudulent scheme.

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?

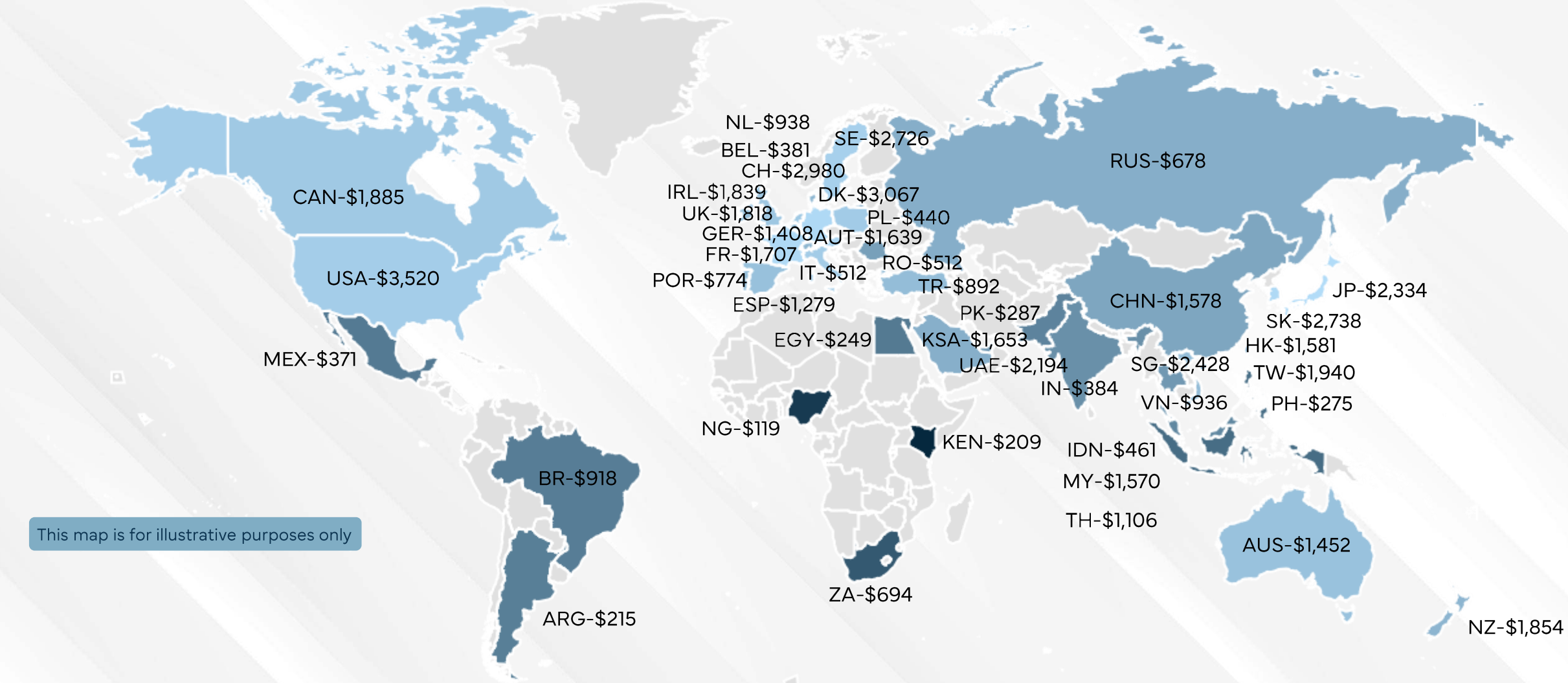
# Revictimization looms large in Belgium, as victims are scammed an average of nearly three times each




People in Malaysia, Hong Kong, and Kenya are at a heightened risk of being repeatedly targeted after a scam.

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

# An estimated US$1.03 trillion has been lost to scams worldwide in the last 12 months

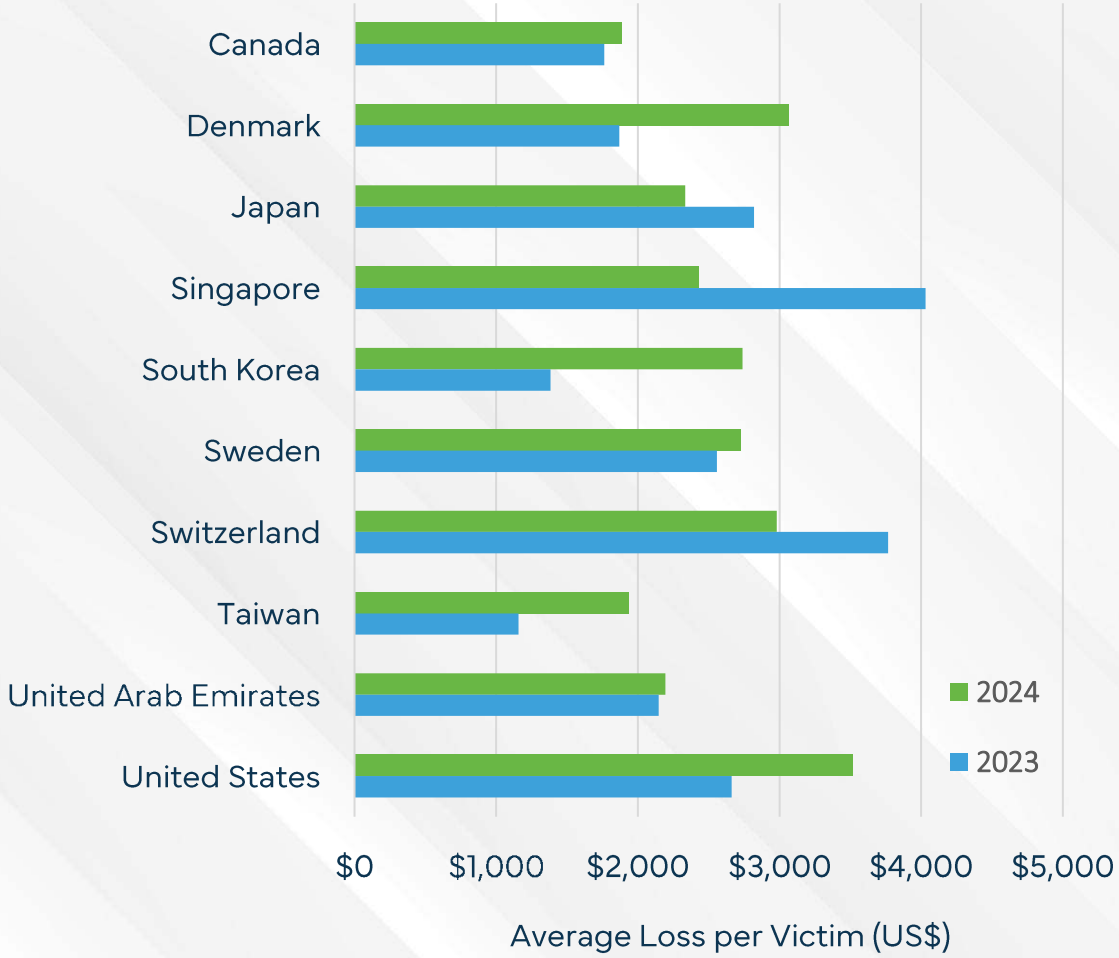



The hardest hit were U.S. citizens, losing an average of $3,520 per capita, followed by the Danish ($3,067) and Swiss ($2,980). By contrast, Nigerians ($119), Kenyans ($209), and Argentinians ($215) lost the least per capita. However, this does not tell the entire story...

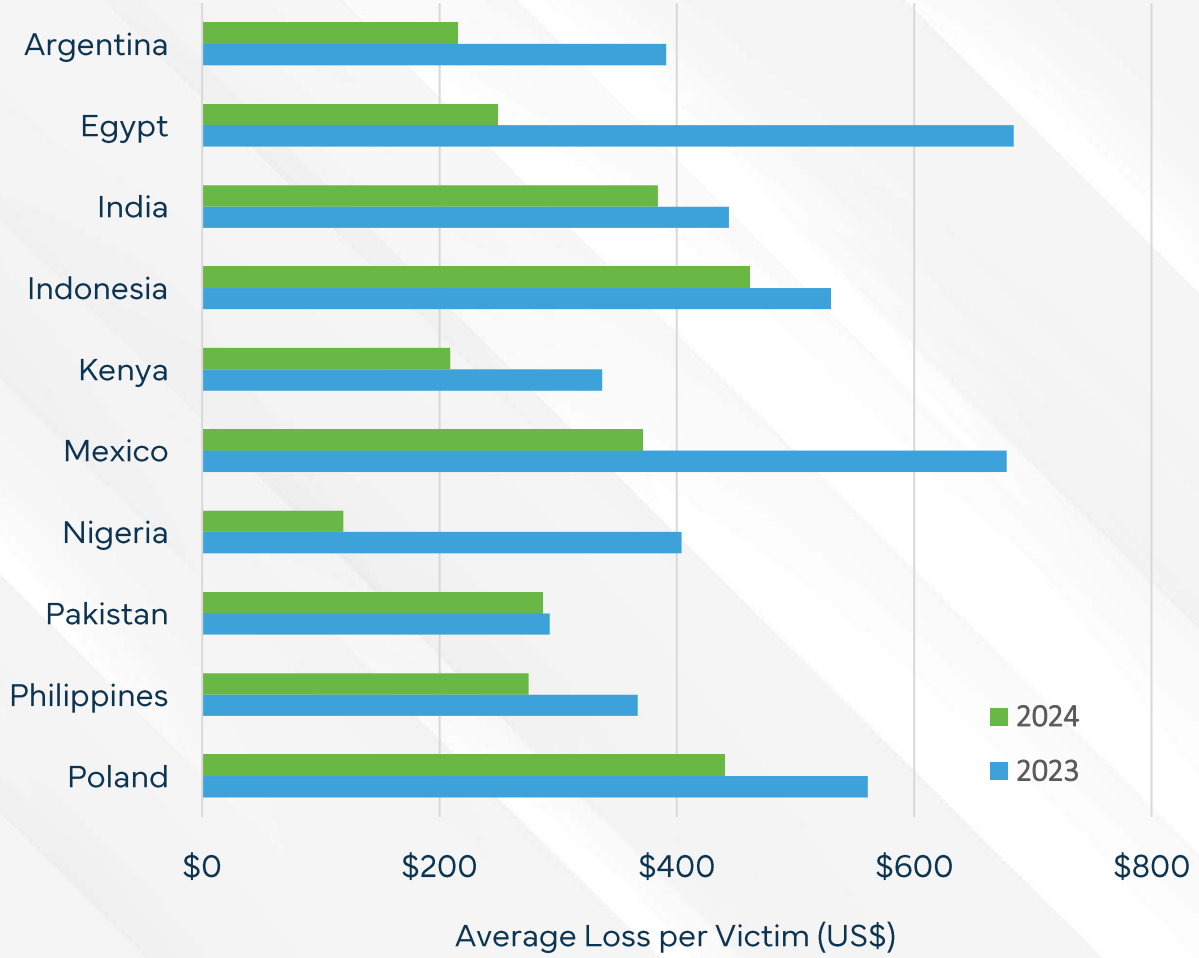
Source: Global State of Scam Report 2023, Global Anti-Scam Alliance

# A pattern emerges as developed nations tend to sustain higher individual losses

## Ten Highest Average Loss per Victim




## Ten Lowest Average Loss per Victim




Despite this, Singapore and Switzerland have seen a sudden drop in their citizen's average loss.

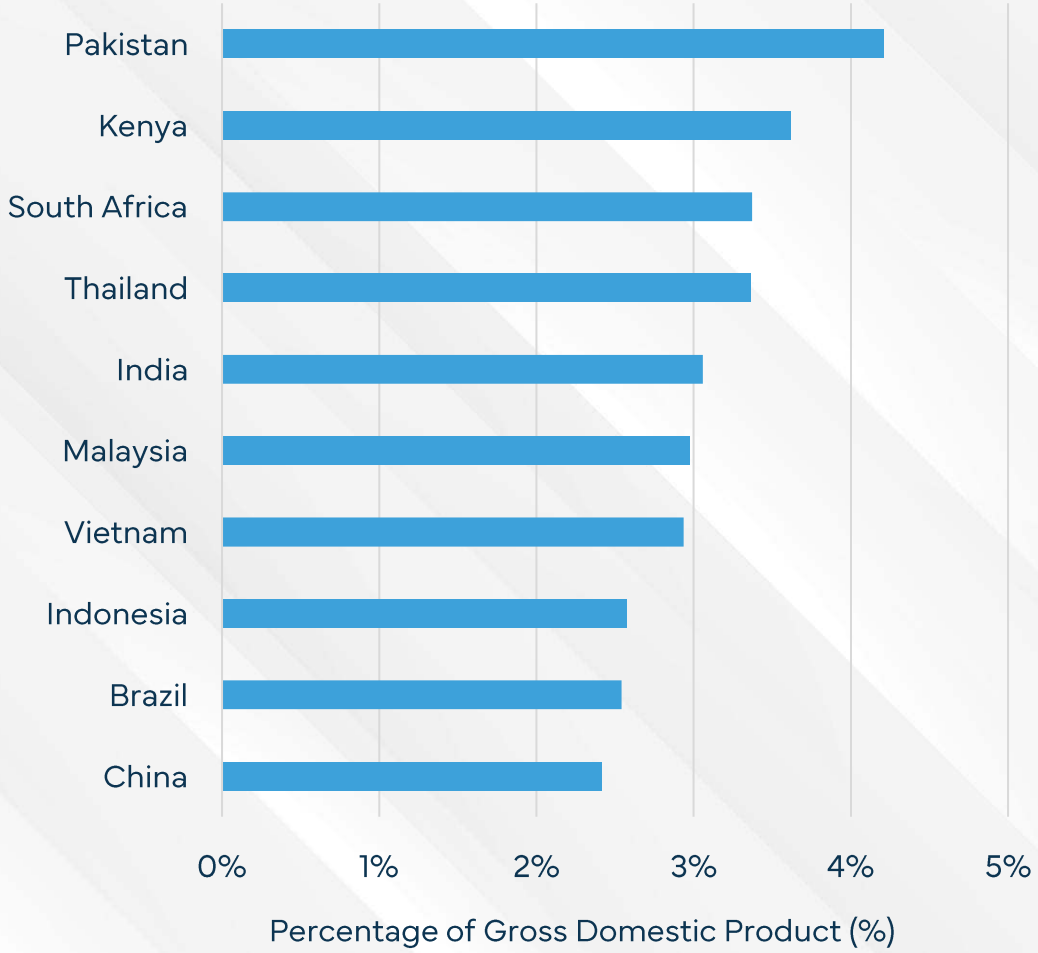
In the last 12 months, in total, how much money did you lose to scams before trying to recover the funds?

# Developing nations are hit hardest with a higher proportion of their GDP being lost to scams than that of developed nations

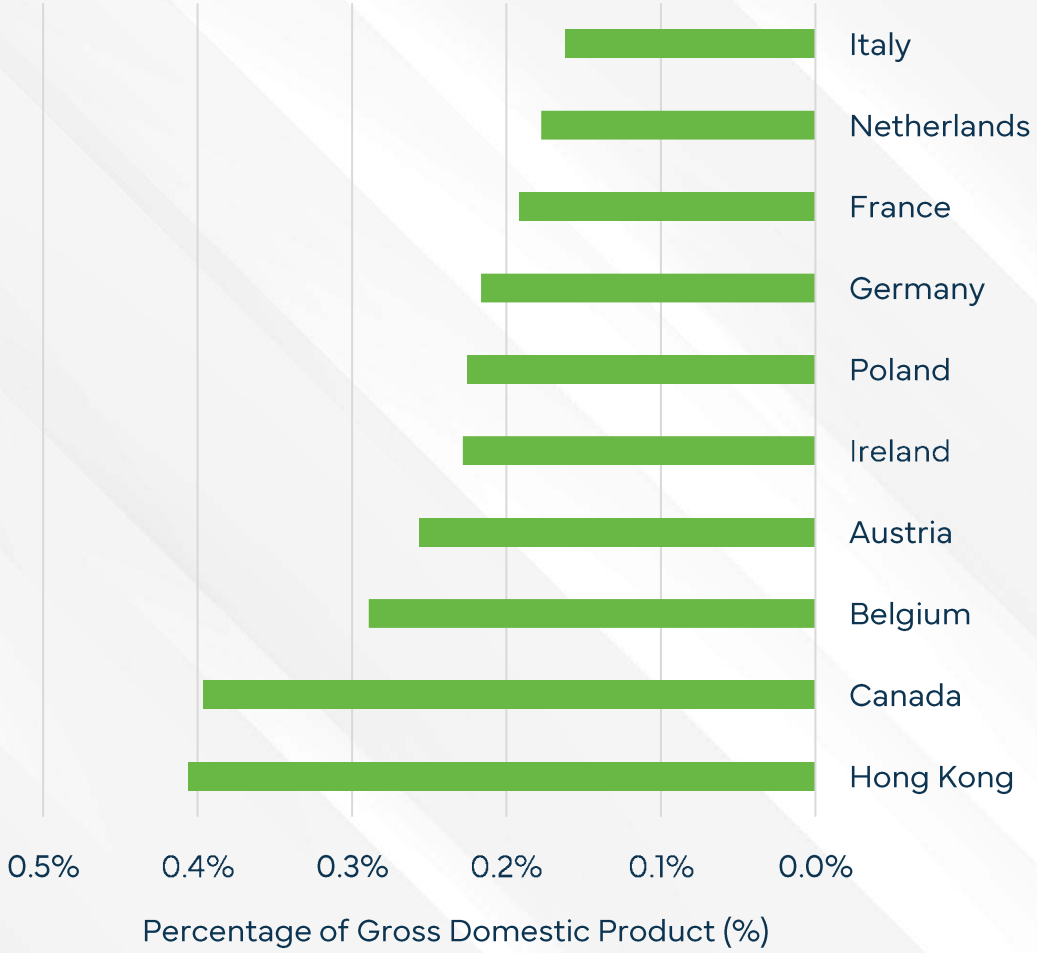
feedzai

GASA
Global Anti-Scam Alliance

## Ten Highest GDP Loss per Country




## Ten Lowest GDP Loss per Country




European countries tend to lose a fraction of their GDP, while there is a visible impact on the economies of Asian and African countries.

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

# Conclusion: The Aftermath of Scams

Banks and payment providers are at the final stage of the scam lifecycle. It is at this stage where illicit attempts to extract money from victims either succeed or fail. It is where scams are most often detected and reported and where the impact of successful scams is felt most.

Financial loss impacts consumers and providers alike. Scams inflict emotional distress on victims—and, to a lesser degree, the providers' own support staff that witness that distress firsthand. Where institutions issue reimbursements, consumers must still ultimately pay through fees or increased charges. This means reimbursement is not an antidote to the scam epidemic. The growing pressure to protect customers from scams, public availability of scam reports, and the emergence of AI-generated fraud attacks are ubiquitous across the globe. Despite some remarkable consistency in the numbers presented in GASA's report compared to last year, there are still some underlying shifts. A lot is being done to reduce the losses. In several countries, the total amount lost, if not the number of cases, is starting to fall.

This is partly due to the efforts of the banks to enforce more intelligent controls and more accurate risk decisions. Banks and payment providers have a significant advantage over criminals—an intimate understanding of their customers. Through AI, banks are starting to use this advantage to protect their customers and build lasting trust. However, significant differences exist, including in the varying approaches adopted by regulators in different countries, which increases the complexity of effective prevention. Another challenge that hampers better scam prevention is the wide variety of global scam reporting and classification methods. Measuring scams is more difficult because each country, industry, and organization has its own definitions. Comparison across sectors, let alone countries, is nearly impossible. The challenge is more significant due to the reluctance of victims to report scams in the first place, as highlighted in this report.

That is why a global organization such as GASA has such an important role to play. More accurate scam risk decisions are dependent on access to more data. Any success by members of GASA or elsewhere to increase the amount of data that is shared confidentially and securely is only going to improve scam controls banks can apply on behalf of consumers. For example, stopping outbound payments that pose a high fraud risk has been the cornerstone of most financial institutions' fraud prevention strategy for years. However, with the emergence of authorized fraud or scams, this is arguably targeting the wrong person. Inbound payments lead directly to the accounts moving illicit funds, as opposed to the genuine account owner making what they believe to be a legitimate payment.

Inbound monitoring provides more opportunities to capture fraud, preventing funds from leaving victims' accounts and identifying mule accounts as funds arrive. Today, many banks don't monitor mule risk in real time. Strategies such as the ability to monitor incoming payments will become more common. We already see a convergence of methodologies paving the way for a standardized approach. Focusing on the mule can also potentially disrupt entire criminal networks, exposing individual bad actors and enabling progress in preventing broader financial crime. We are witnessing the mainstreaming of generative AI underpinning the risk & regulatory landscape. Fraudsters who have already seen an increase in purchase scam success now have access to AI, which is so powerful that it can create images, scripts, videos, and voices in seconds. 2 years ago, this wasn't possible. Today, we all see the headlines of millions lost in a 5-minute video call.

As fraudster attacks begin to leverage AI, the volume of customers fooled will increase, meaning more fraudulent payments will be processed. Therefore, fraud rates will rise. It's a natural consequence. However, the power of GenAI's ability to reproduce rapidly is also its weakness. With the right technology, banks can monitor attack patterns and more quickly detect similarities that are more obvious in replicated attempts.

Banks cannot fight this battle alone. True disruption requires collaboration across the ecosystem —social media giants, ISPs, tech titans, and telcos must join the fight. Coordinated takedowns and intelligent data exchange are needed to outsmart criminals who operate without borders. Proactive protection of consumers and financial integrity will define the future of security. Anticipating, educating, preventing, and detecting threats is the only way forward.

Nuno Sebastião
Co-Founder, Chairman, and CEO
Feedzai

feedzai

# 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.

**Feedzai** is the market leader in fighting financial crime with AI. We're coding the future of commerce with today's most advanced risk management platform powered by big data and machine learning. Feedzai built the world's first RiskOps platform specifically engineered and patented to combat financial crime. Our customers spend less time thinking about risk and more time growing their business.

# Methodology

1. Survey Administration:

- **Tool Used:** Pollfish.com
- **Methodology:** Random Device Engagement (RDE), a successor to Random Digit Dialing (RDD), delivers surveys through popular mobile apps to a neutral, unsuspecting audience. This approach minimizes premeditated survey-taking biases.

2. Incentives and Fraud Prevention:

- **Incentives:** Non-monetary perks, such as extra lives in games or access to premium content.
- **Fraud Prevention:** Advanced AI and machine learning technologies to remove biased responses and enhance data quality.

3. Data Correction and Estimation Challenges:

- **Statistical Corrections:** Adjustments made based on the general demographic distribution within each country to account for potential biases in age or education level.
- **Estimation Limitations:** Outliers were removed as needed, and losses under one bitcoin were not included due to reporting constraints.
- **Estimated Amount Lost:** To calculate the total amount lost per country, we followed these steps:
    - Percentage of Participants Losing Money: We first determined the total number of participants who reported losing money in each country. This number was then divided by the total number of survey participants from that country to get the percentage of people who lost money.
    - Estimating the Total Number of Scam Victims: We multiplied the percentage of participants who lost money by the total population over 18 years old in that country. This gave us an estimate of the total number of scam victims in each country.
    - Calculating the Average Amount Lost: The average amount lost per person was calculated by averaging the reported losses from participants in each country, after removing any outliers that could skew the results.
    - Total Money Lost: Finally, we multiplied the estimated total number of scam victims over 18 years old by the average amount lost in their respective country. This provided the estimated total financial loss due to scams for each country.
    - This methodology ensures that the data reflects a reliable estimate of the financial impact of scams across different populations and regions.
- **Survey Respondents by Country:** The data presented in this report has been carefully weighted to account for differences in population size across the countries surveyed. This ensures that the findings accurately reflect the relative prevalence of scams in each country, irrespective of the total number of respondents. The weighting process allows for a more balanced comparison between countries with varying population sizes.
- **The total number of individuals who completed the survey varies by country, with respondent numbers as follows:** Argentina: 1,000 | Australia: 1,000 | Austria: 500 | Belgium: 880 | Brazil: 1,322 | Canada: 1,360 | China: 1,000 | Denmark: 556 | Egypt: 1,000 | France: 2,000 | Germany: 2,000 | Hong Kong: 511 | India: 1,000 | Indonesia: 1,000 | Ireland: 1,000 | Italy: 1,000 | Japan: 921 | Kenya: 1,000 | Malaysia: 1,202 | Mexico: 1,000 | Netherlands: 1,012 | New Zealand: 1,071 | Nigeria: 1,000 | Pakistan: 1,000 | Philippines: 1,000 | Poland: 1,000 | Portugal: 1,000 | Romania: 1,000 | Russian Federation: 1,000 | Saudi Arabia: 500 | Singapore: 1,199 | South Africa: 1,000 | South Korea: 708 | Spain: 1,000 | Sweden: 574 | Switzerland: 269 | Taiwan: 5,003 | Thailand: 9,630 | Türkiye: 1,000 | United Arab Emirates: 1,964 | United Kingdom: 2,000 | United States: 2,500 | Vietnam: 647.

Of the 94,954 people approached with the Global State of Scams 2024 survey, fully completed surveys were submitted by 58,329 individuals across 42 countries.

4. Additional Data Sources:

- **Inhabitants per country:** Worldometers.info
- **Currency conversion:** Xe.com
- **Internet penetration:** Wikipedia
- **GDP Estimate 2024:** Wikipedia

5. Translation and Localization:

- **Procedure:** Each survey was translated and localized by a human to align with the official or most commonly spoken language of the target country.

6. Inspirational Reference:

- **Study:** The methodology was partly inspired by the findings of DeLiema, M., Mottola, G. R., & Deevy, M. (2017) in their pilot study to measure financial fraud in the United States (SSRN 2914560).

# About the authors

**Jorij Abraham** has been active in the Ecommerce industry since 1997. From 2013 to 2017, he has been Research Director at Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and the Ecommerce Foundation.

Nowadays, Jorij is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.

**Sam Rogers** is GASA's Director of Research & 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. Having left industry behind in 2023, Sam leads the GASA research and marketing team in the collection of survey data, the final State of Scams reports, and creation of supporting analytical literature.

**Luka Koning** is a data specialist at Kennispunt Twente, with extensive experience in research and data analysis. Prior to this, he served as a researcher at the University of Twente, focusing on fraud victimization in the Netherlands, cybercrime, and moral behaviour. Luka has contributed to various research projects, including collaborations with the Netherlands Enterprise Agency and the development of social science insights for cybersecurity.

**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

feedzai 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
Capital One
feedzai
Gogolook
Google
SCAMADVISER
Meta
TREND MICRO
Match Group

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

feedzai

## Disclaimer

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