



# Global State of Scams

## 2025 REPORT

INSIGHTS

LEARN MORE



# 73% of the global population is confident to recognize scams but 23% lost money



**Jorij Abraham**

MANAGING  
DIRECTOR



## About GASA

The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

This study of 46,000 adults across 42 markets reveals that seven in ten adults globally have encountered a scam in the last 12 months, with 13% encountering a scam at least once a day. Nearly three fifths of adults globally have experienced a scam, with prevalence highest in Oceania and South America.

## Widespread Financial Impact

Shopping scams (54%), investment scams (48%) and unexpected money scams (48%) are of the most common types of scams globally. Furthermore, almost a quarter of adults claim to have had money stolen by scammers in the last year, with wire or bank transfers (29%) and credit card payments (18%) being the most common channels through which scammers receive funds.

## Yet Reporting Often Falling Short

70% adults globally have had a scam experience in the last year, with scam exposure most common in Oceania, South America and Africa. Of those who have encountered a scam, 70% have reported it at least once, with over a third claiming that no action was taken by the platform after reporting it. 27% of adults globally have never reported a scam encounter, with uncertainty over who to report to (36%) being the main barrier, followed by the perception that it was not important because they had not lost any money (35%).

## While Stress and Tension Rise

Globally, the impact of scams is both financial and emotional, with 17% of adults experiencing a drop in confidence and 14% claiming to have heightened tension and stress in their family unit as a result of being scammed. More than two thirds of those who have experienced a scam found the experience to be stressful, particularly those in South America, Africa and the Middle East. However, the scam experience has also resulted in an increased vigilance of scams (36%) and a reduction in normal spending behaviour (14%).

## And Encourages Greater Caution

93% of adults globally claim to take at least one step to verify if an offer is legitimate or not. However, many often rely on methods that are less effective such as checking for spelling and grammar errors (27%); looking for reviews on the same website (24%) and checking if the company is on social media (21%).

Despite nearly three quarters of adults globally feeling confident in their ability to recognise a scam, scams remain prevalent, with many scam victims losing money and a significant proportion never reporting their encounters.

# From Transactions to Intent: The New Front Line in Fraud



**Nuno Sebastião**

CEO



## About Feedzai

Feedzai is the world's first end-to-end financial crime prevention platform, protecting people and payments with AI-native solutions that stop fraud and financial crime. Leading financial institutions trust Feedzai to manage critical risk and compliance processes, safeguarding trillions of dollars of transactions while improving the customer experience and protecting the privacy of everyday users.

Feedzai is committed to providing its clients with the most advanced and effective solutions and expertise while driving innovation and advancing the fight against financial crime.

Every day, millions of people around the world receive a scam call, text, or message. Most people ignore them, but some don't. What happens next isn't determined by how clever the scammer is, but by whether the victim's bank is ready to see the payment for what it really is. Not just a transfer of money, but a decision with intention behind it.

A payment on its own is like a photograph: a single frame, frozen in time. Look deeper at the intention behind it, and the still image becomes a moving picture, rich with depth and context.

Intention matters because scams rarely leave a clear fingerprint in the payment itself. The fraud is hidden in the circumstances around it. It shows up in the gap between what a trusted customer has always done and what they are suddenly persuaded to do. That's where the danger lies, and that's where the chance to intervene lives.

Scam prevention isn't simple work. It sits at the crossroads of technology, criminal collaboration, authorized transactions, and human psychology. Criminal groups trade data, tools, and increasingly even AI models. Victims, meanwhile, authorize payments believing they are making a sound decision. Fraud happens in real time, denying banks the luxury of second chances. When behavioral patterns are combined with transaction data, it becomes possible to tell whether a customer is acting as themselves, or whether their intention has been hijacked. That recognition has become the new front line of fraud prevention.

But intention, by itself, is not enough. The other part of the challenge is scale.

No single bank can stand against this tide on its own, and no single industry can either. Organized crime doesn't operate in silos. It spreads tactics and kits across borders with alarming speed. A single breach or malware campaign can ripple across dozens of institutions. What begins as a stolen password today can become a drained account tomorrow.




The response has to match that level of coordination. Banks, payment providers, and cybersecurity teams need to share insights as easily as fraudsters trade exploits. If we wait until an attack hits the payment system, it's already too late.

The path forward is clear. AI cannot remain a niche tool used by a few; it must become the standard. Institutions that take this step will stop scams more effectively, and they will earn something that is hard to win but easier to lose: the trust of customers who know their bank is watching out for them in ways they could never manage. That is how today's threats are turned into tomorrow's strength.



# The Global research surveyed 46,000 respondents across 42 markets

Markets by Region | Sample size

## North America:

-  Canada | 1000
-  United States | 2500
-  Mexico | 1000





## South America:

-  Argentina | 1000
-  Brazil | 1000




## Europe:

-  Austria | 1000
-  Belgium | 1000
-  Denmark | 1000
-  France | 2000
-  Germany | 2000
-  Ireland | 500
-  Italy | 1000
-  Netherlands | 1000
-  Poland | 1000
-  Portugal | 1000
-  Romania | 1000
-  Spain | 1000
-  Sweden | 1000
-  Switzerland | 1000
-  United Kingdom | 2000

## Africa:

-  Egypt | 1000
-  Kenya | 1000
-  Nigeria | 1000
-  South Africa | 1000



## Middle East:

-  Saudi Arabia | 1000
-  Türkiye | 1000
-  United Arab Emirates | 1000

## Asia:

-  China | 1000
-  Hong Kong | 1000
-  India | 1000
-  Indonesia | 1000
-  Japan | 1000
-  Malaysia | 1000
-  Pakistan | 1000
-  Philippines | 1000
-  Singapore | 1000
-  South Korea | 1000
-  Taiwan | 1000
-  Thailand | 1000
-  Vietnam | 1000

## Oceania:

-  Australia | 1000
-  New Zealand | 1000

# Who we spoke to Globally

**Sample size** | 46000 people

**Audience** | Adults aged 18+ living in each market

**Quotas** | Quotas were used throughout fieldwork to ensure the sample was nationally representative of the adult population in each market on age, gender and region

**Weighting** | Nationally representative of adult population in each market

**Methodology** | 15-minute online survey

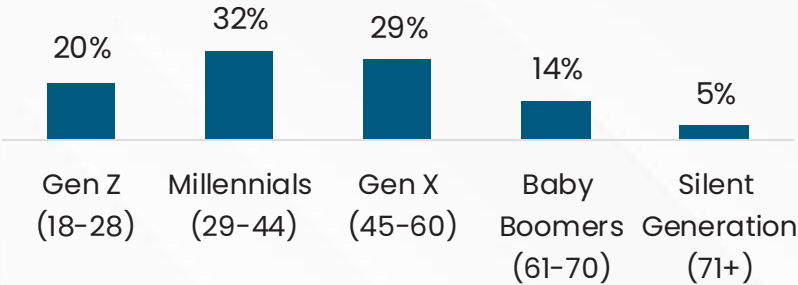
**Sample source** | Online research panel

Base: All respondents Globally (46,000)

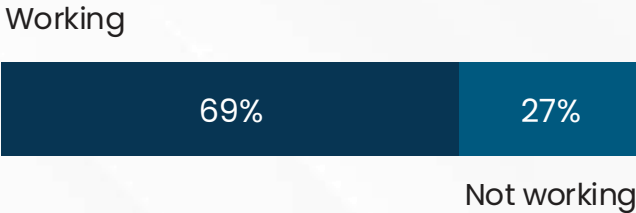
## GENDER



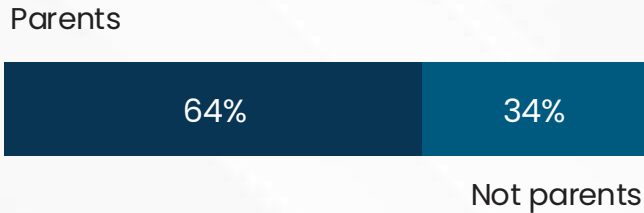
## GENERATION / AGE



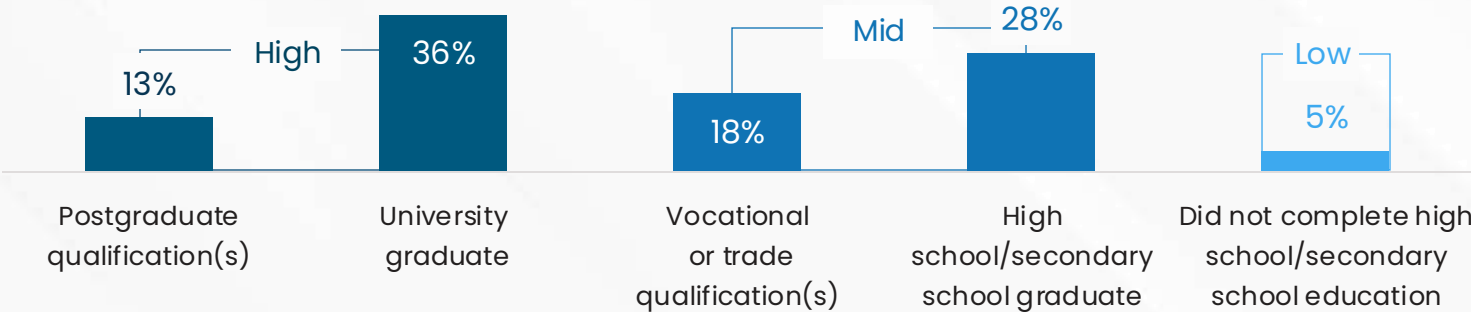
## WORKING STATUS



## PARENTAL STATUS



## EDUCATIONAL STATUS



# Key **Global** findings

## PREVALENCE OF EXPERIENCING A SCAM IN LAST 12 MONTHS

57%

Of adults **Globally** claim to have had a scam experience in the last 12 months  
Amongst this group, **Shopping scam** (54%) is the most common type of scam experienced

\*An experience, whether successful or not for the scammer

## PREVALENCE OF LOSING MONEY TO SCAMS IN LAST 12 MONTHS

23%

Of adults **Globally** went on to have money stolen by scammers in the last 12 months

This rises to 41% in South America and Africa

## VALUE LOST TO SCAMS

**\$442 Billion**

(estimated, as seen on methodology)

Has been lost to scams worldwide in the last 12 months

Funds are most commonly sent via Wire or bank transfer (**29%**) and credit card payment (**18%**)

## PERCEIVED RESPONSIBILITY TO PROTECT PEOPLE FROM SCAMS

35%

Of adults **Globally** feel it is the responsibility of **Public service or Commercial organisations** to protect people from scammers, primarily the online platform used by the scammer (**13%**) or the government (**13%**)

## IMPACT OF SCAMS ON VICITM

69%

Of adults **Globally** who were scammed felt very or somewhat stressed by the experience

**36%** say they will be more vigilant of scams as a result

## PREVALENCE AND OUTCOME OF REPORTING TO PAYMENT PROVIDER

74%

Of adults **Globally** who were scammed did report the scam to the payment service

**30%** were able to at least partly recover the money





Throughout the report, you can click the 'Home' icon to return to this page

# The research covered the following **key topics**

## SCAM PREVALENCE

How many people experience scams?  
What are the most common scam types experienced? And what is the value stolen by scammers?

## EXPERIENCE OF BEING SCAMMED

How frequently do scams occur?  
Which payment channels are used to send funds?

## SCAM REPORTING

Are scams reported? If so, what are the outcomes of reporting scam encounters? If not, what are the barriers?

## SCAM IMPACT

What impact do scams have on victims' lives, stress and wellbeing?

## PREVALENCE OF SCAM ENCOUNTERS

How frequently are scams encountered? And on what platforms?

## SCAM PREVENTION

What self-prevention tactics to consumers use to identify scams?  
How are public and commercial organisations' seen in their responsibility and performance in preventing and resolving scams?

## ABOUT THE REPORT

To find out more about the report and its authors

## ABOUT THE AUTHORS

Click to  
navigate to  
sections



# From Social Media to Sophisticated Scams: The Need for United Action



**Ravi Govindaraju**

HEAD OF TRUST & SECURITY

**JPMorganChase**

## About JPMorganChase

With a history tracing its roots to 1799 in New York City, JPMorganChase is one of the world's oldest, largest, and best-known financial institutions—carrying forth the innovative spirit of our heritage firms in global operations across 100 markets. We serve millions of customers and many of the world's most prominent corporate, institutional, and government clients daily, managing assets and investments, offering business advice and strategies, and providing innovative banking solutions and services.

Fraud and scams pose significant threats to consumers' financial, emotional, and physical security. According to the FTC, Americans are estimated to lose as much as \$158 billion per year. Scams initiated on social media are particularly attractive to criminals due to several factors, including the ease of impersonation, a false sense of security, and the ability to quickly create new accounts, thereby scaling their scam operations.

As artificial intelligence continues to advance, the risk of more sophisticated schemes increases. Criminals can exploit these technologies to target and scam society's most vulnerable individuals with highly realistic impersonations and threats. It is important to remember that criminals manipulate people long before money changes hands. This means there are multiple missed opportunities to detect and stop criminals before they contact consumers and money is sent out.

Robust cooperation across all sectors – technology, telecommunications, government, law enforcement and finance – is crucial to effectively combat and mitigate emerging challenges. Each sector plays a vital role in safeguarding consumers. At JPMorganChase, we are committed to making investments and contributing our firm's resources to protect people from scams. Through our collaboration with GASA, we aim to strengthen partnerships and work towards effective, cross-industry solutions that will safeguard communities worldwide.



A blurred background image on the left side of the slide shows a woman wearing a light-colored hijab and a white shirt, holding a blue credit card in her right hand. A laptop keyboard is visible in the lower left foreground.

# Scam prevalence

How many people experience scams? What are the most common scam types experienced? And what is the value stolen by scammers?



## Scam experiences more prevalent in South America and Oceania

Prevalence of experiencing a scam in last 12 months

**57%**  
of adults Globally  
have had a scam  
experience in the  
last 12 months

66% ↑

North  
America

U.S. – 70%

72% ↑

South  
America

Argentina – 74%

53% ↓

Europe

Ireland – 79%

68% ↑

Africa

Kenya – 83% — Highest market(s) per region

51% ↓

Middle East

United Arab  
Emirates –  
54%

53% ↓

Asia

Philippines – 65%

73% ↑

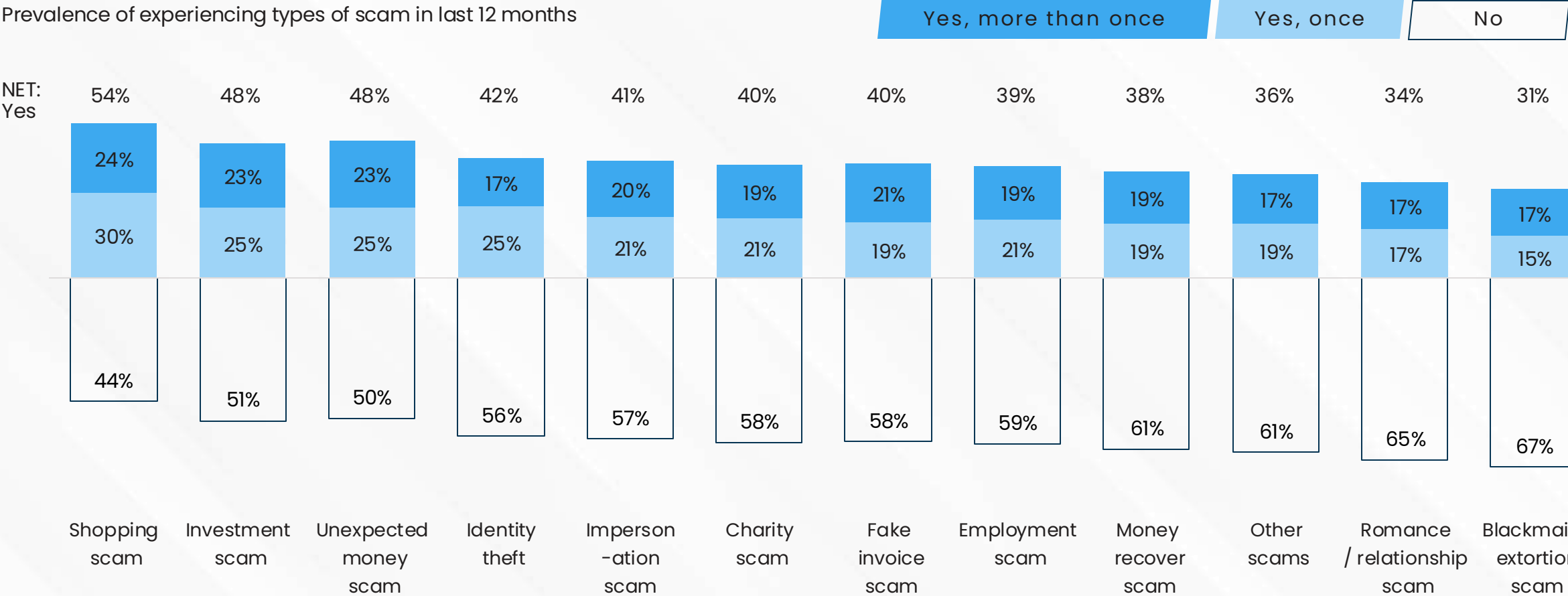
Oceania

Australia – 74%



# Shopping, unexpected money & investment scams are the most experienced type of scam globally, affecting around half of scam victims

Prevalence of experiencing types of scam in last 12 months





## With fraudsters employing various methods to deceive consumers globally



"Ordered a product, that I thought was a reliable company, the product was never delivered"

**Shopping scam, U.S.**



"An email arrived about a provincial tax debt that was too high. Therefore I was in red status, as a debtor, and I paid one of the instalments"

**Fake invoice, Argentina**



"I purchased products online, the products did not arrive and from research I later discovered that it was a scam. I reported the matter to the bank who refunded me the amount paid"

**Shopping scam, Italy**



"Some called telling me he has sent money and was suppose to pay hospitals bill so he wanted me to reverse the money back to him"

**Impersonation scam, Kenya**



"The fraudster called and gave me my bank account information and told me that he would update it. I gave him the information and he stole the amount"

**Unexpected money scam, United Arab Emirates**



"Impersonating as a lhdn officer [Lembaga Hasil Dalam Negeri] saying that I have an outstanding tax that needs to be paid in full as the so called company that is registered under my name never paid taxes"

**Investment scam, Shopping scam, Impersonation scam, Charity scam, Malaysia**



"My card was used for a subscription that I did not pay for and when I contacted the company they tried to say I subscribed myself"

**Shopping scam, New Zealand**

# Fraud and scams are no longer just a consumer protection issue



**Kate Griffin**

DIRECTOR FINANCIAL  
SECURITY PROGRAM



## About the Aspen Institute

The Aspen Institute is a global nonprofit organization committed to realizing a free, just, and equitable society. Founded in 1949, the Institute drives change through dialogue, leadership, and action to help solve the most important challenges facing the United States and the world.

Fraud and scams are no longer just a consumer protection issue—they are a national security crisis. At the Aspen Institute Financial Security Program, we track how transnational criminal organizations use fraud and scams to generate billions in illicit revenue annually, funding everything from drug cartels to human trafficking to cyberattacks. The threat is systemic, and the response must be as well.

Every day, scammers steal more from American families. This is not petty crime—it is industrialized theft. In 2023 alone, over 21 million U.S. adults were targeted directly or through a family member. These are working parents, seniors, veterans—people who believe they're answering a call from their bank or clicking a link from a trusted institution. Veterans and service members are especially vulnerable.

Fraud doesn't just hurt financially. For many, it's a deeply personal violation. Scammers exploit trust—posing as loved ones, official agencies, or familiar brands—to confuse and deceive. The emotional toll is severe. Two-thirds of scam victims report suffering long-term emotional impacts, including anxiety, depression, and PTSD.

What makes this threat more alarming is who's behind it. Transnational criminal groups like the Jalisco New Generation Cartel, the Zhao Wei Organization, and North Korea's Lazarus Group run large-scale scam operations. Some operate entire call centers with the express purpose of "crippling the economy of America", according to eye-witness reports. These aren't isolated fraudsters—they are strategic, well-funded actors deliberately targeting American consumers and institutions. Even modest progress would have a huge impact. Reducing fraud and scams by just 25% would deny these international criminal organizations nearly \$40 billion in annual revenue.

In the U.S., interested stakeholders must work together to elevate it to the national priority that it is. Federal efforts remain fragmented. Agencies lack the tools to share intelligence swiftly, while victims often don't know where to turn. Meanwhile, financial institutions and private-sector organizations—many of whom are making meaningful efforts to educate and protect their customers—are too often left to fight this alone.

We need a national strategy to bring coherence to this fight. That's why the Aspen Institute Financial Security Program has convened a National Task Force on Fraud and Scam Prevention. We've brought together leaders from consumer protection, technology, finance, and law enforcement to design a real plan of action. One that strengthens cross-sector coordination, updates laws, and gives every American better protection and recourse when targeted. This isn't just about crime prevention. It's about restoring trust in our economy, defending vulnerable populations, and cutting off a major funding source for global criminal networks.



## Funds lost due to scam activity is particularly prevalent in South America and Africa

Prevalence of losing money to a scam in last 12 months

**23%**  
of adults Globally  
went on to **have**  
**money stolen by**  
**scammers** in the  
last 12 months

24%

North  
America

Mexico – 34%

41% ↑

South  
America

Argentina – 44%

20% ↓

Europe

Ireland – 27%

41% ↑

Africa

Kenya – 53% — Highest  
market(s)  
per region

25%

Middle East

United Arab  
Emirates – 33%

19% ↓

Asia

Pakistan – 39%

22%

Oceania

New Zealand – 23%

Q13. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it. Base: All respondents Globally (46000), North America (4500), South America (2000), Europe (17 500), Africa (4000), Middle East (3000), Asia (13000), Oceania (2000)

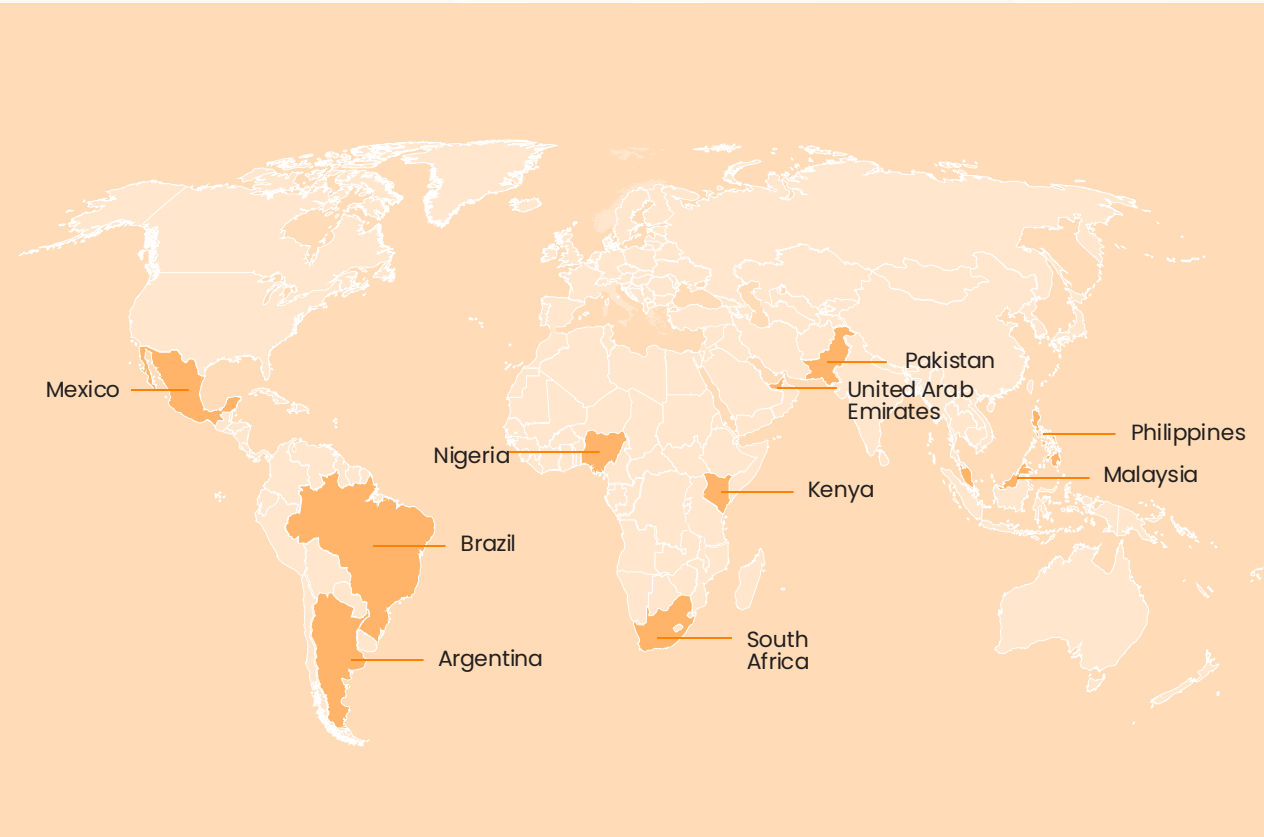




# Although scam susceptibility appears globally dispersed, the likelihood of financial loss is notably higher in developing countries

Top ten markets most vulnerable to **being scammed**

Top ten markets most vulnerable to **losing money to scams**





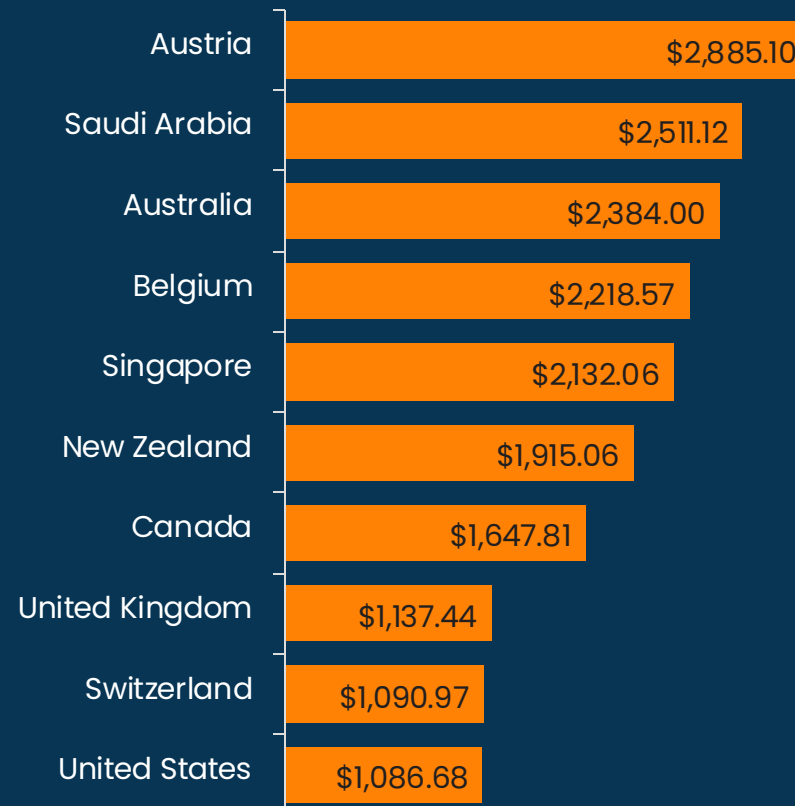
An estimated  
**\$442 Billion** has been  
 lost to scams  
 worldwide in the last 12  
 months...

Value lost to scams, see methodology page.

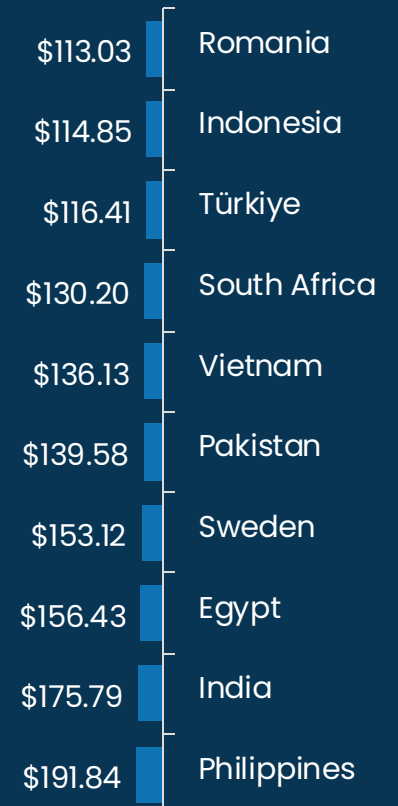
Q13. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it. Base: those who lost money (10732) \*NB, markets without sufficient base size for those losing money to scams have been omitted from this list

## Among those that lost money, Austria has the highest average loss, with Saudi Arabia and Australia on 2<sup>nd</sup> and 3<sup>rd</sup> place

Ten **highest** average loss\*



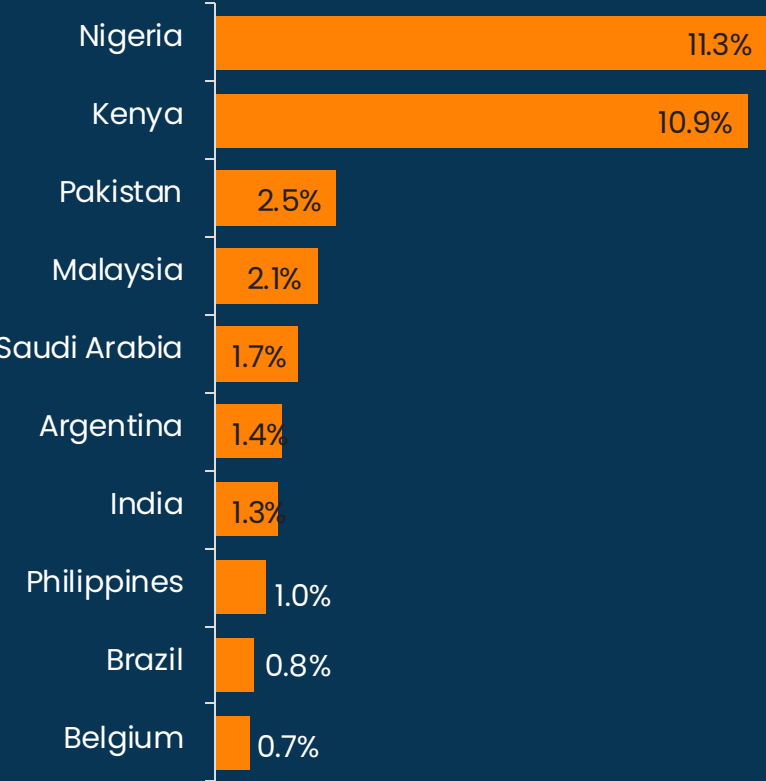
Ten **lowest** average loss



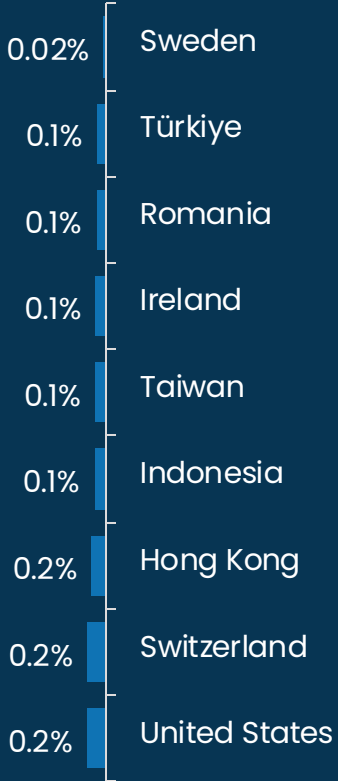


# When viewed in a wider context, developing nations have a higher proportion of their GDP stolen to scams

Ten **highest** GDP loss per country



Ten **lowest** GDP loss per country



Click the image below to access the interactive map and view data by market



Q13\_USD. In the last 12 months, in total, how much money did you lose to scams? Please include the total amount of money lost, regardless whether you managed to partially or fully recover it. Base: All respondents (46000)

# Cross-sector collaboration: a key component in the fight against scams



**Pooja Paturi**

DIRECTOR DIGITAL PAYMENT  
FRAUD PREVENTION



## About the Canadian Bankers Association

The Canadian Bankers Association is the voice of more than 60 domestic and foreign banks operating in Canada and their more than 280,000 employees and it continues to provide governments and others with a centralized contact to all banks on matters relating to banking in Canada. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

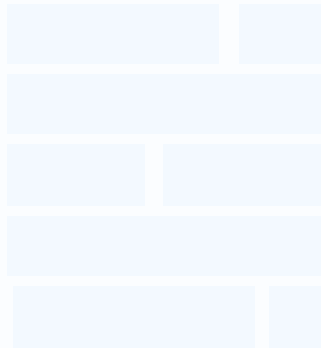
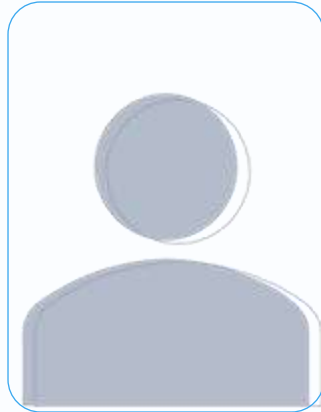
Cross-sector collaboration is essential in the fight against scams, and no single organization—public or private—can tackle the growing sophistication of scams on its own. The Canadian Bankers Association is a strong proponent of working together through voluntary cross-sector collaboration to better protect the public and disrupt the criminal networks that benefit from scams.

Telecommunications providers, digital platforms, financial institutions, law enforcement, and government agencies each have an important role to play if we are to succeed in preventing scams. Technology companies can detect and prevent scams through AI-driven content moderation and platform abuse detection. Telecoms can flag spoofed calls, while banks can flag suspicious transactions. Law enforcement can act on intelligence, and government can help support collaboration. However, improved real-time data sharing, joint response protocols, and broad education campaigns that help empower consumers are all needed in this fight.

Collaboration isn't just a best practice, it's a necessity. When sectors align their efforts, we create a stronger, more resilient scam prevention ecosystem. The public deserves a united front against scams, and it's up to all of us to deliver it.



Versus **23% globally**, those susceptible to being scammed and losing money are...



From a **younger generation**

27%  
GEN Z

26%  
MILLENNIALS

From a **low GDP country...**



Low GDP

30%

Have **children**



Parents

27%

Have a **high level of education**



High  
Education

26%

...Specifically **South America or Africa**



South  
America 41%



Africa 41%



# Scams are hitting hard across the globe though who's affected and how varies widely

## Scam prevalence summary:

In the past 12 months, a majority of individuals across the globe report having been scammed. Regional differences are stark: South America, Oceania, North America, and Africa see the highest incidence, while Europe, the Middle East, and parts of Asia report fewer cases. The leading scam types across all regions are shopping, investment, and “unexpected money” scams.

Approximately a quarter report a financial loss from the scam, which equates to nearly half of those who experienced a scam. Regions like South America and Africa show both high scam exposure and frequent monetary loss. Meanwhile, in Oceania, scam reports are relatively high but reports of financial loss are notably lower, hinting at more awareness.

Looking at a market level, developing markets like Kenya and Nigeria show highest proportions reporting financial loss. However, it's not a straightforward picture, countries like the UAE also appear in the top ten, and Denmark tops the list in Europe for reports of money lost, despite being one of the region's strongest economies.

When it comes to the average amount lost, wealthier nations top the list. Japan sees the highest average losses despite having one of the lowest scam report rates. Australia and Saudi Arabia also see higher than average financial hits among those who do lose money. But if you look at losses relative to GDP, developing countries are taking a disproportionately large hit (Nigeria and Kenya in particular).

Beyond geography, certain groups are more vulnerable to financial loss from scams. Younger generations, who are more likely to be shopping online or encountering investment “opportunities” via social media, are particularly at risk. Parents and those with higher education levels are also more likely to lose money, challenging the common assumption that lower education equals higher vulnerability.



# Combating scams in Brazil: a challenging scenario, but with improvements on the way



**Rafael Henrique Martins Fernandes**

PUBLIC PROSECUTOR & CHIEF PLANNING  
OFFICER AT THE PUBLIC PROSECUTION  
OFFICE OF THE STATE OF MINAS GERAIS



## About MPMC

The Public Prosecutor's Office of the State of Minas Gerais (MPMG) is an autonomous public institution dedicated to defending citizens' rights and the interests of society. Its mission rests on three pillars: safeguarding the legal order, protecting the democratic regime, and upholding inalienable social and individual rights.

Brazil continues to face a serious challenge from digital scams, which remain widespread and damaging. Yet, several recent initiatives show that progress is underway.

In the justice system, state Public Prosecutors' Offices in Minas Gerais (MPMG) and Mato Grosso (MPMT) proposed the creation of a dedicated registry for electronic fraud, which has been welcomed by the National Council of the Public Prosecutor's Office (CNMP). By clearly distinguishing between digital and conventional fraud, authorities can make more accurate diagnoses—an essential step toward building effective countermeasures. In parallel, negotiations between the CNMP and GASA aim to strengthen prosecutorial networks, boosting awareness and enabling a more integrated response.

Regional initiatives highlight the same trend. The Public Prosecutor's Office in Piauí (MPPI) launched the "Alerta Digital" project, inspired by Minas Gerais' "Chegando Junto" program. Through TV and local media, the project publishes educational reports on common scams, helping to empower citizens through awareness and prevention.

"The financial sector is also acting. The Central Bank of Brazil issued a new regulation ordering banks not to carry out transactions when fraud is suspected and it is preparing new tools to make it harder to open fraudulent bank accounts often used to launder illicit funds. It is also developing an Enhanced version of the Special Refund Mechanism (MED) for Pix instant payments, designed to make it easier to block suspicious transactions and return stolen Money to victims.

On the legal front, the Federal Supreme Court (STF) recently reinterpreted the Brazilian Civil Rights Framework for the Internet. Digital platforms can now be held liable under the Consumer Protection Code if they fail to take effective measures against fraudulent content—a ruling that could drive stronger platform accountability. Meanwhile, in the legislative branch, Bill No. 3,237 proposes a National System to Combat Electronic Fraud. If approved, it would fill an institutional gap and bring Brazil closer to international best practices, such as National Anti-Scam Centers.

While Brazil's scam landscape still demands sustained attention and effort, these judicial, financial, and legislative measures collectively signal that the country is moving toward a more coordinated, preventive, and resilient response to online fraud.

A photograph of a woman with long blonde hair and glasses, seen in profile from the chest up. She is looking out a window with a view of a city skyline. The image is partially obscured by a dark blue diagonal overlay on the right side of the slide.

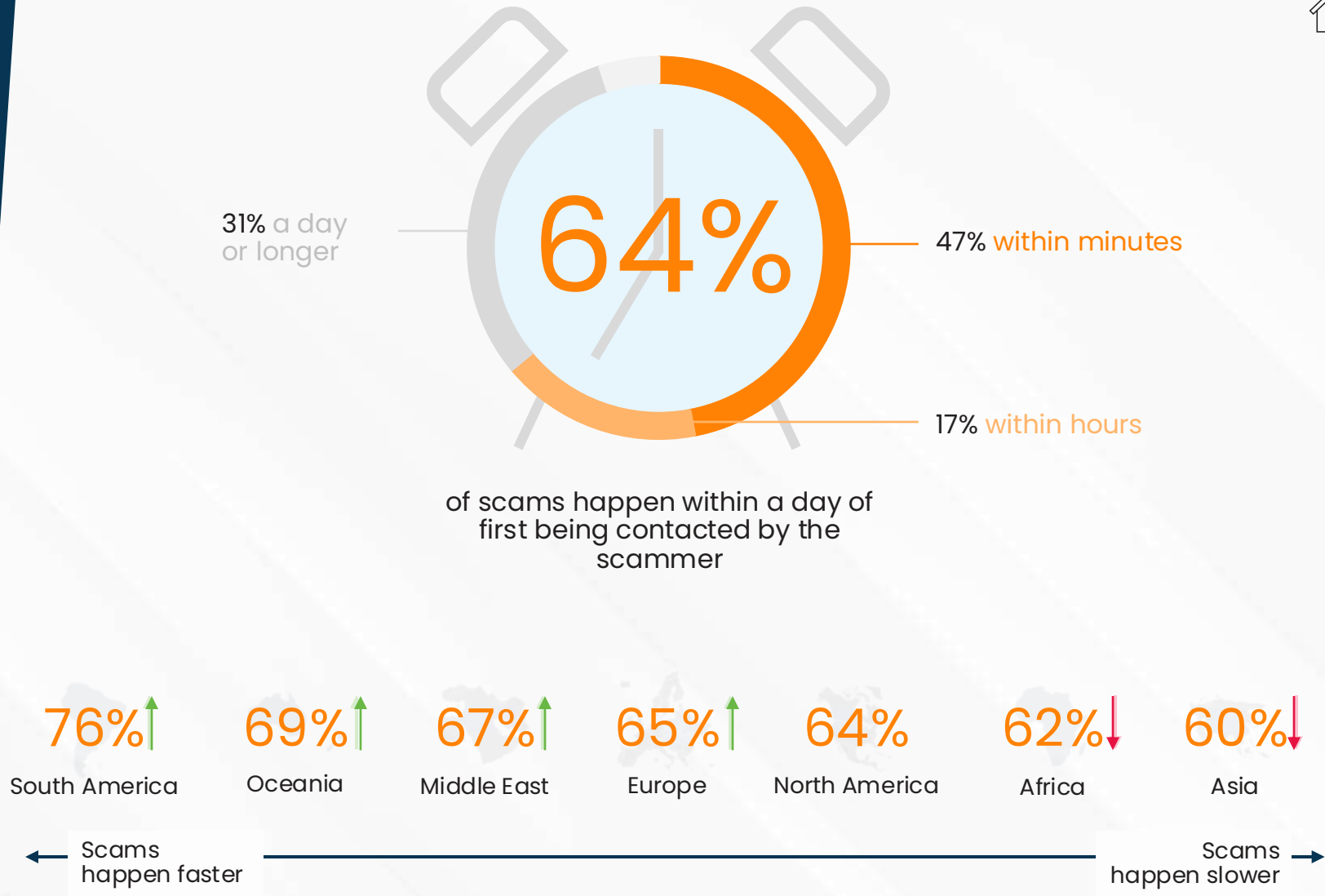
# Experience of being scammed

How frequently do scams occur? Which payment channels are used to send funds?



Globally, just under two thirds of scams happen within a day of first being contacted by the scammer

Proportion of scams that happen within a day

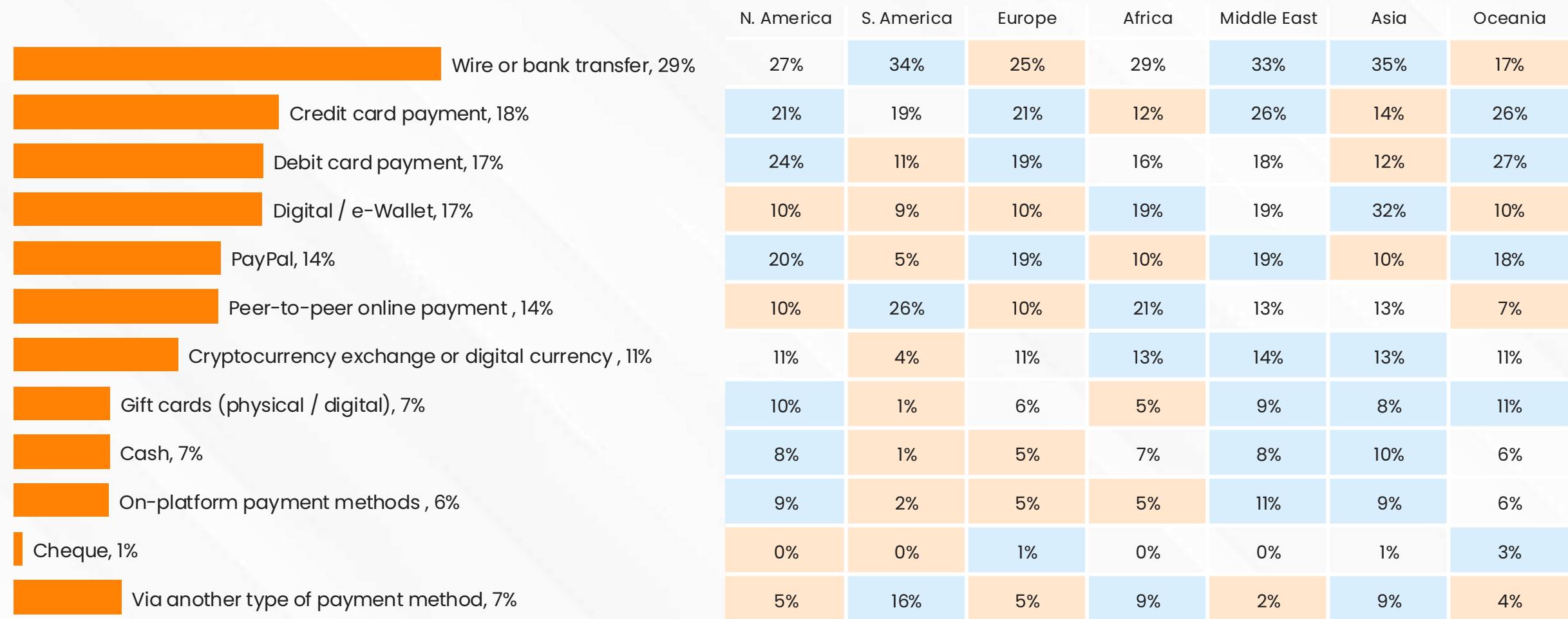


Q10. Thinking about the most recent time you were scammed, how long did it last? Please think about from the first time you heard from the scammer until the last time you were in contact with the scammer. Base: All respondents who have been scammed (26817), North America (2996), South America (1435), Europe (9419), Africa (2778), Middle East (1535), Asia (7187), Oceania (1467)



# Wire or bank transfer is the most common method of transferring money to scammers, particularly in South America, the Middle East and Asia

Payment channels scammers received the payment



Q14. How did the scammer receive your money? Base: All respondents who have been scammed and lost money (11447), North America (1071), South America (1109), Europe (3623), Africa (1714), Middle East (791), Asia (2699), Oceania (440)



# Victims are quick to transfer money via wire or bank transfer

## Experience of being scammed summary:

Globally, nearly two-thirds of scams are over within a day of first contact, with almost half saying it took just minutes from the initial approach to the last interaction. This pattern is especially strong in South America, where countries like Argentina and Brazil see over half of scam victims falling victim within minutes.

The most common method used to steal money is via wire or bank transfer. This means many victims are sending money to a scammer almost immediately after being contacted, raising concerns about the tactics being used. The speed suggests scammers are leveraging urgency and emotional pressure to prompt fast decisions. Indeed, victims reported being urged to clear fabricated debts and send money for hospital or tax bills.

# Stolen Data, Smarter Scams: Europol Warns of AI-Driven Cybercrime



**Emmanuel Kessler**

HEAD PREVENTION &  
OUTREACH EUROPOL



## About Europol

Europol is the European Union Agency for Law Enforcement Cooperation. Our main goal is to achieve a safer Europe for the benefit of all EU citizens. Headquartered in The Hague, the Netherlands, we assist the 27 EU Member States in their fight against serious international crime and terrorism. We also work with many non-EU partner states and international organisations.

The 2025 Europol IOCTA report highlights a chilling reality: stolen personal data – the core enabler of today’s cybercrime ecosystem – is more valuable than ever. Criminals exploit generative AI to produce convincing phishing, deepfake, and Business Email Compromise attacks, while Initial Access Brokers monetise breach credentials through crime-as-a-service networks. Abuse of the Domain Name System (DNS) further enables these schemes, giving scammers rapid, low-cost infrastructure to host fake platforms, mask their identities, and evade takedowns.

Europol’s fight against scams is exemplified in a recent multinational operation dismantling a network behind a fake online trading platform – a multimillion-euro investment scam defrauding over 100 victims. Coordinated by Germany with support from five countries and facilitated by Europol’s virtual command post, the effort shows how swift, cross-border intelligence sharing disrupts fraud before it scales.

Prevention must target both technology and governance. This means awareness campaigns that demonstrate AI-driven deception, regulatory measures embedding “privacy, security, and DNS abuse mitigation by design” in online services, and robust e-governance frameworks to enforce accountability across jurisdictions. Finally, scalable digital literacy programs– reaching parents, educators, and vulnerable groups – can foster critical verification skills and healthy scepticism. The European Cybercrime Centre (EC3) promotes policy development and fosters public-private-partnership with global organisations, registries and registrars to empower the global community in combating scams more effectively and significantly reduce their impact on society.

By uniting law-enforcement action, industry safeguards, and citizen vigilance, we can close the gaps scammers exploit.





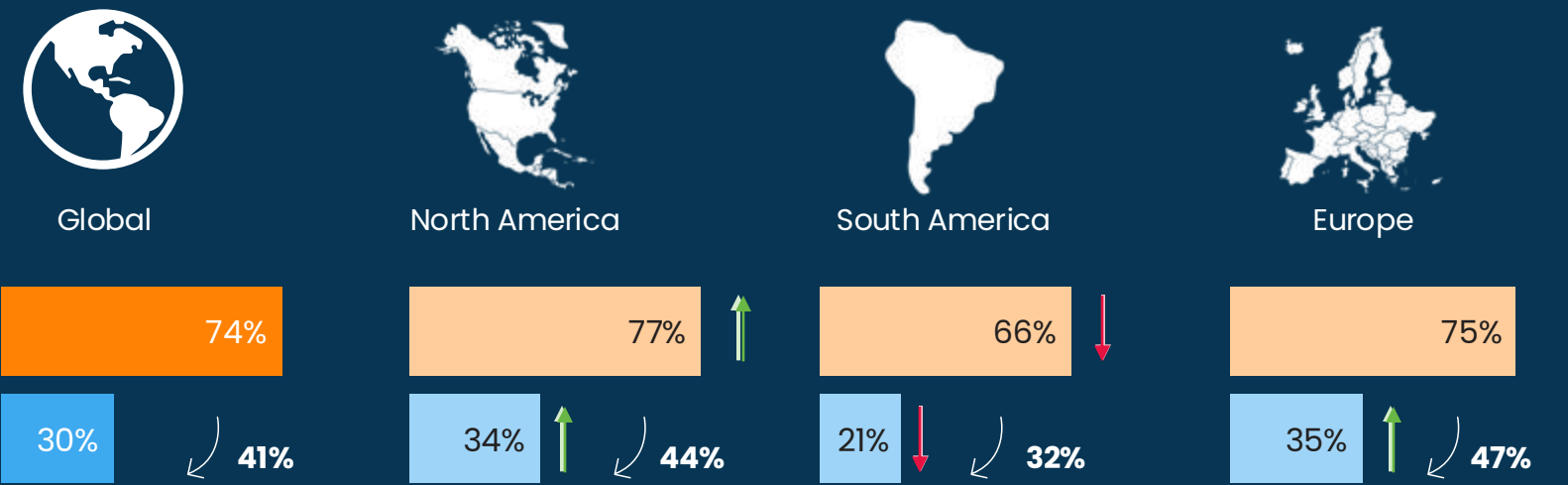
# Scam Reporting

Are scams reported? If so, what are the outcomes of reporting scam encounters? If not, what are the barriers?



# Reporting and financial recovery is more prevalent in the Middle East and Oceania

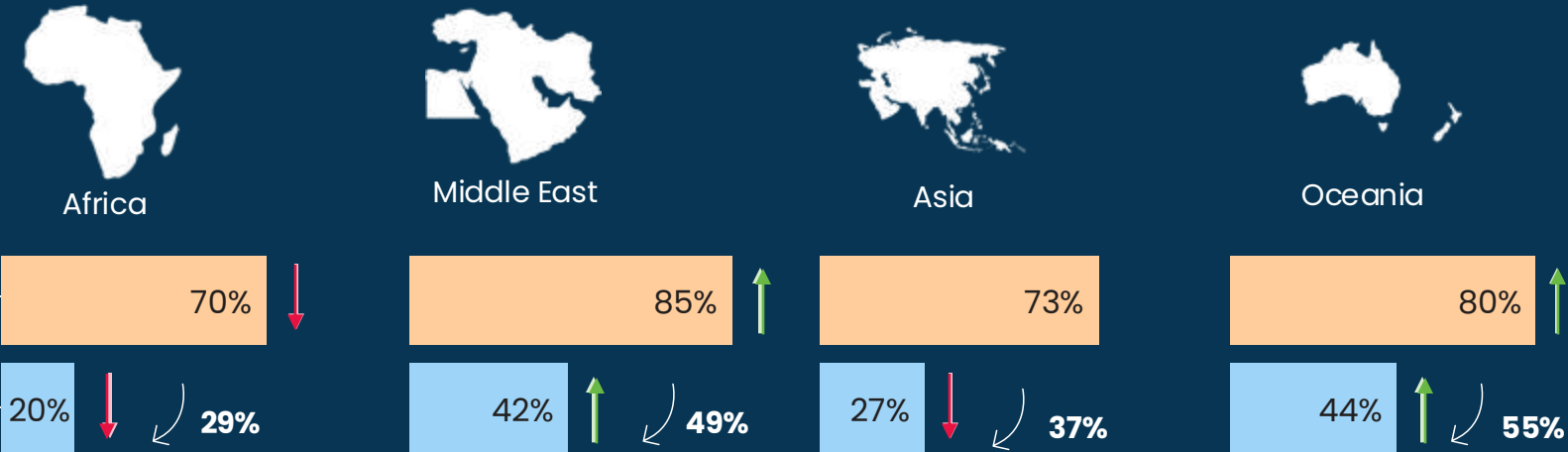
Prevalence of reporting scams to payment provider & if money was at least partially recovered



Conversion from reporting to partially recovering funds

Yes – reported the scam to the payment service used to send money to scammer

Money at least partially recovered

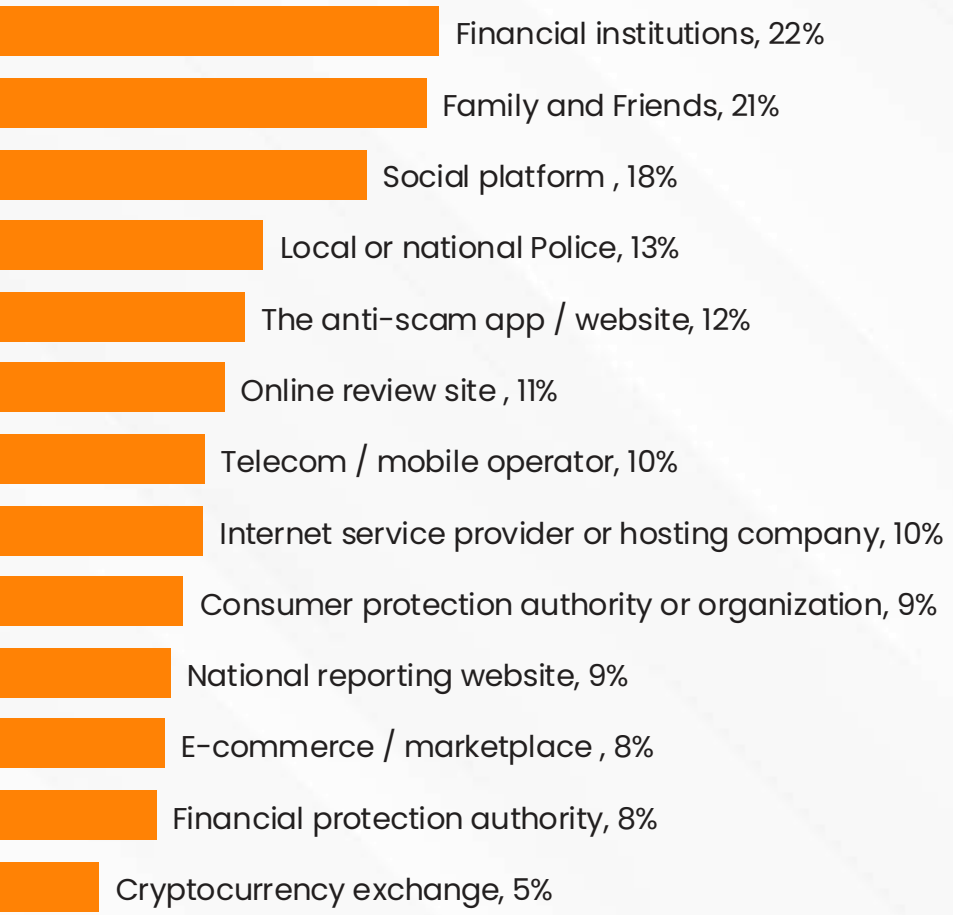


Q15. Did you report the scam to the payment service that was used to send your money to the scammer? Base: All respondents who have been scammed and lost money (11447), North America (1071), South America (1109), Europe (3623), Africa (1714), Middle East (791), Asia (2699), Oceania (440)



# Overall, scams are reported to the greatest variety of channels in the Middle East and Asia

Channels / organisations scams reported to



	N. America	S. America	Europe	Africa	Middle East	Asia	Oceania
Financial institutions	25%	31%	22%	25%	26%	16%	27%
Family and Friends	16%	28%	18%	27%	21%	26%	15%
Social platform	17%	19%	15%	25%	17%	22%	17%
Local or national Police	11%	12%	12%	12%	18%	16%	9%
The anti-scam app / website	11%	9%	10%	13%	14%	16%	11%
Online review site	11%	11%	9%	15%	13%	13%	9%
Telecom / mobile operator	8%	6%	8%	16%	15%	13%	8%
Internet service provider or hosting company	11%	6%	8%	13%	13%	12%	11%
Consumer protection authority or organization	10%	9%	8%	9%	14%	11%	6%
National reporting website	8%	9%	7%	6%	13%	10%	8%
E-commerce / marketplace	8%	9%	8%	6%	12%	10%	6%
Financial protection authority	8%	5%	6%	9%	12%	10%	6%
Cryptocurrency exchange	4%	3%	4%	7%	8%	6%	4%



## Those in North America, Europe and Oceania were more resistant to reporting their scam

Prevalence of not reporting scams in the last 12 months

**20%**  
of those  
experiencing a  
scam in the last 12  
months did not  
report it to anyone

23% ↑

North  
America

Canada – 29%

20%

South  
America

Argentina – 24%

23% ↑

Europe

Sweden – 33%

14% ↓

Africa

South Africa – 33% — Highest market(s) per region

14% ↓

Middle East

Türkiye – 19%

18% ↓

Asia

South Korea – 26%

25% ↑

Oceania

Australia – 25%

# Fighting Fraud Together: A Global Call for Empathy and Action



**Nicholas Court**

DIRECTOR PRO TEMPORE,  
INTERPOL FINANCIAL CRIME AND  
ANTI-CORRUPTION CENTRE



INTERPOL

## About Interpol

The world's largest police organization, INTERPOL assists law enforcement in its 196 member countries to combat transnational crime. Guided by four core functions, it provides technical and operational support via a high-tech infrastructure to meet 21st-century challenges. The General Secretariat in Lyon operates around the clock, serving as a central contact for National Central Bureaus and enabling secure cross-border investigations through I-24/7 and a suite of colour-coded international notices.

We know that fraud is not simply a crime with a financial impact. Individual victims often experience emotional distress that can leave them feeling isolated from their friends and family — and in the most serious cases, these feelings can cost lives. This is one reason we launched the *Words Matter* campaign last year, encouraging law enforcement officials and the wider public to recognize that certain language can stigmatize and dehumanize victims, and imply that fraud is their fault. Criminals commit fraud; victims do not.

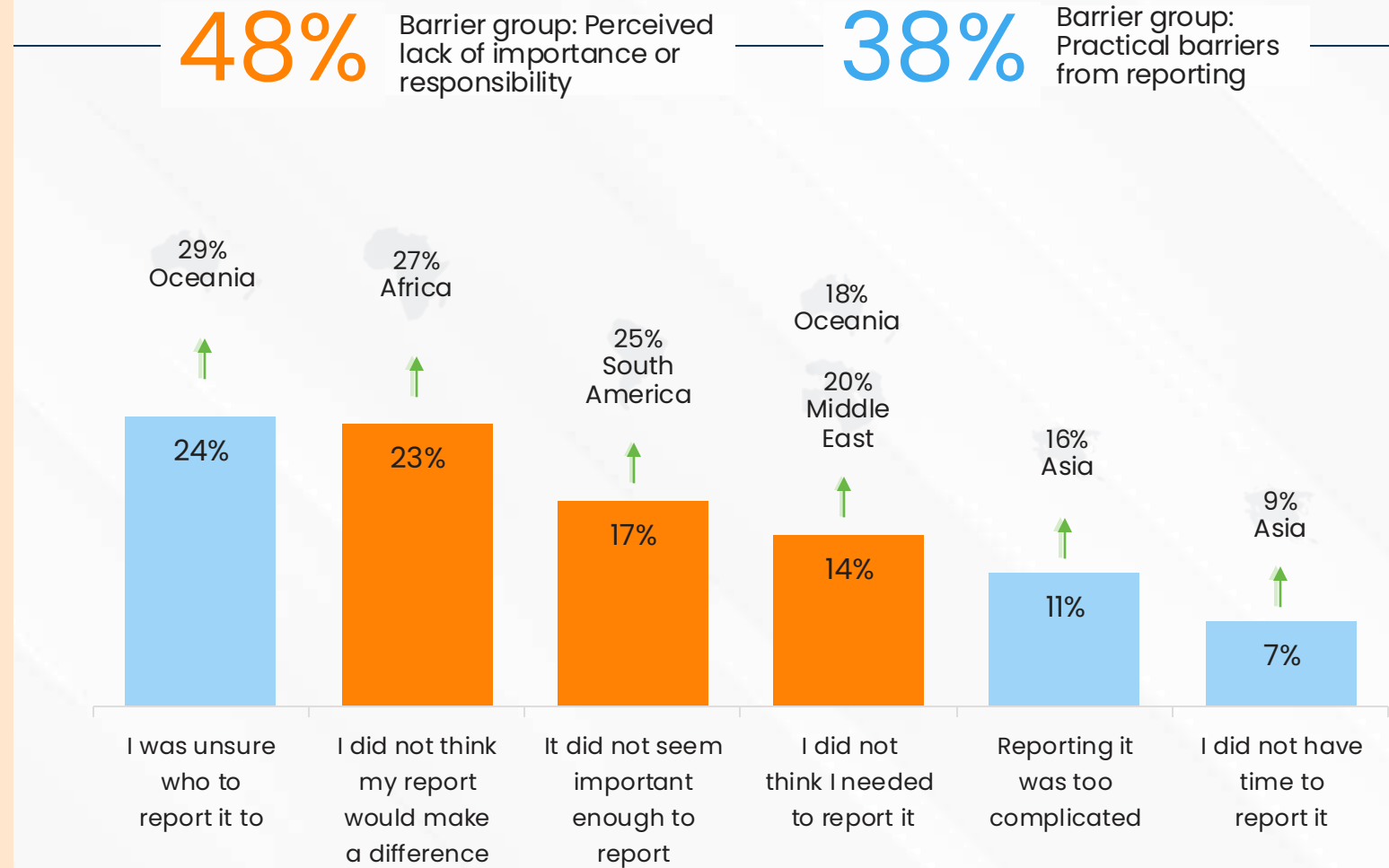
Both GASA and INTERPOL recognize that fraud is a crime with severe consequences, and I am pleased to support this important publication, which helps us all better understand the scale of the threat we are facing together. Criminals are making full use of modern technologies and operating at scale, including through so-called scam call centres. They are also learning from one another — as seen during a recent operation conducted by Namibian authorities and supported by INTERPOL, in which scores of people were rescued from forced labour to commit fraud and hundreds of digital devices were seized and analysed.

As much as criminals develop and adapt, the same is true of the global law enforcement community. Countries from all regions of the world, regardless of geopolitical challenges, are coming together more frequently to share information and intelligence on criminal networks and the methods they use. We are at the heart of this cooperation. Throughout 2026, we will continue to support our member countries through operational activity, knowledge sharing, and international engagement, with the aim of making the world a more difficult place for criminals — and a safer one for people and businesses across the globe.



## Barriers to reporting scams are primarily driven by a **perceived lack of responsibility** or a **functional reason**

Barriers to reporting scams – top 6

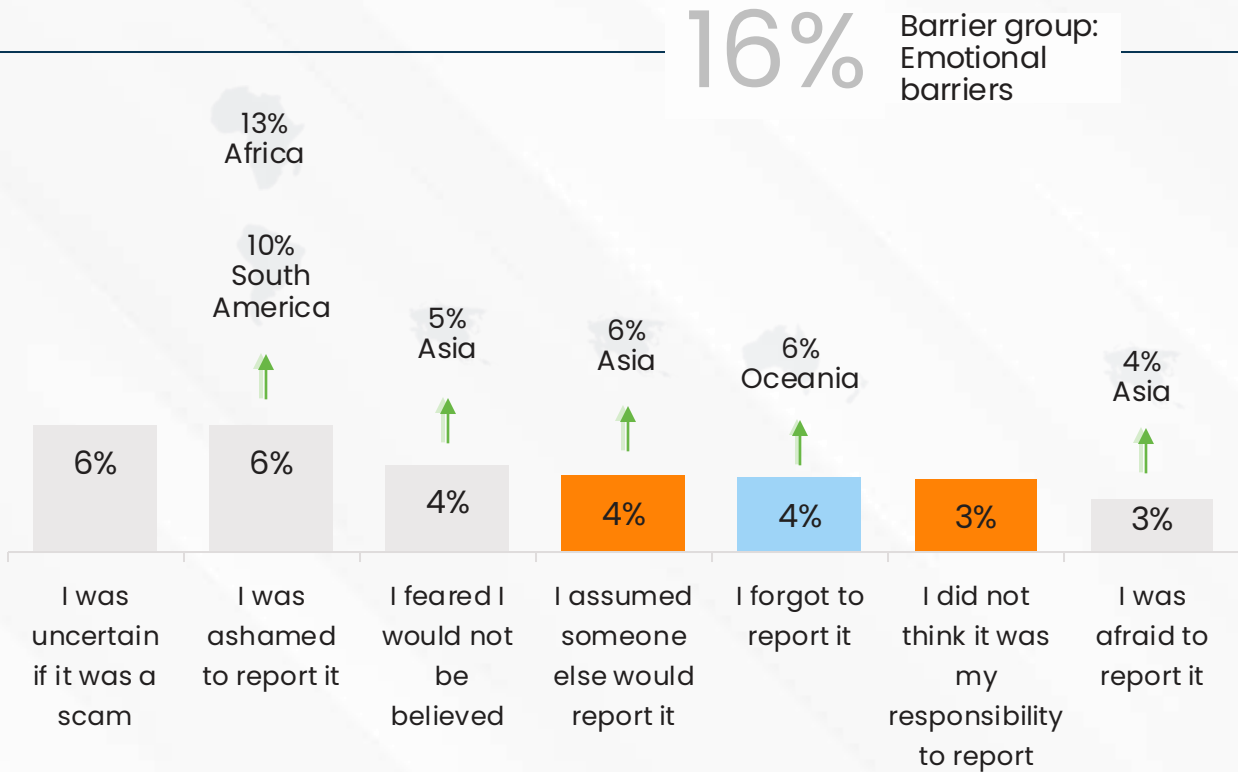






# However, emotional barriers are also at play, particularly in Africa, South America and Asia

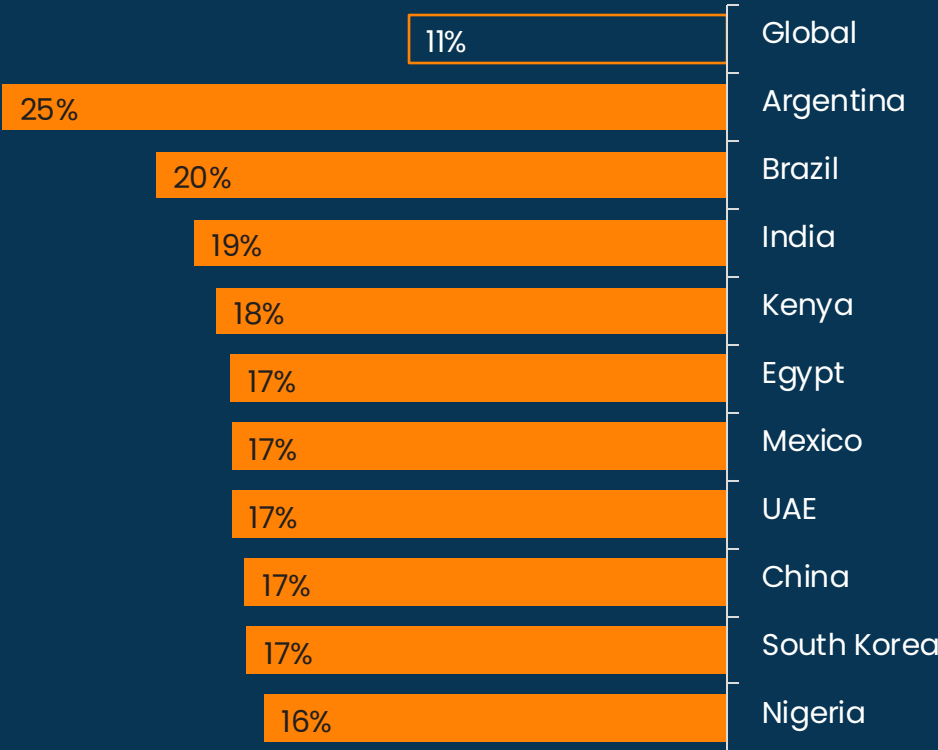
Barriers to reporting scams – bottom 7



Q22. Why didn't you report the scam? Base: Respondents who did not report the scam (5333), North America (691), South America (243), Europe (2172), Africa (406), Middle East (196), Asia (1271), Oceania (354)

# Which is unsurprising given the prevalence of 'blaming the victim for being careless' in these markets

% saying they experienced victim blaming after their scam experience – ten highest markets



Q18. How has the scam(s) impacted you and your family? Base: All respondents who have been scammed (26817), North America (2996), South America (1435), Europe (9419), Africa (2778), Middle East (1535), Asia (7187), Oceania (1467)



# Scam reporting: The role of recovery and shame

## Scam reporting summary:

Globally, around three-quarters of scam victims report the incident to the payment service used. However, money is only partially or fully recovered in just under a third of cases.

Reporting and recovery are more common in the Middle East and Oceania, and lowest in South America, particularly in Argentina, where two-thirds of victims don't report the scam at all.

The first-place people turn to is typically their financial institution, but friends and family are almost just as likely to be told. Only around one in ten victims report the scam to local or national police.

The main barriers to reporting are a lack of understanding around how to report or a belief that doing so won't make any difference. In Argentina, where reporting is among the lowest, resolution rates are also particularly poor when victims do attempt to report.

Emotional barriers also play a role, especially in Africa, South America and Asia. Many victims said they felt ashamed. Again, Argentina stands out, with the highest number of people reporting shame around being "careless" as a lasting emotional impact, possibly reinforcing reluctance to report.

# The Escalating Threat Of Scams



**Laura Quevedo**

EVP, FRAUD AND DECISIONING  
SOLUTIONS



## About Mastercard

Mastercard powers economies and empowers people in 200+ countries and territories worldwide. Together with our customers, we're building a sustainable economy where everyone can prosper. We support a wide range of digital payments choices, making transactions secure, simple, smart and accessible. Our technology and innovation, partnerships and networks combine to deliver a unique set of products and services that help people, businesses and governments realize their greatest potential.

Scams are evolving at an unprecedented pace, driven by AI, social engineering, and cross-border criminal networks. From investment scams and shopping scams to deepfake impersonation scams, the tactics are more sophisticated and the stakes higher than ever.

Threat actors are shifting from card phishing to e-commerce scams by setting up fraudulent merchant accounts and fake websites to sell non-existent goods or services, deceiving consumers and then selling those credentials on the dark web.

Given the varied nature of each scam, banks can reduce losses with targeted strategies. Many shopping scams are high volume, low value attacks that can be detected using automated tools. More complex scams such as investment scams often require significant investigation and direct engagement with the consumer.

Valuable lessons can be drawn from markets such as the United Kingdom and Australia, where reported losses have been reduced through the implementation of new technologies to identify and flag potential risks in conjunction with national programs focused on consumer education and awareness.

Network-level technologies have shown strong results. For instance, in the United Kingdom, banks collaborate in data-sharing consortia to analyze real-time payments and apply AI-powered scoring services to protect customers. Similar global services are being developed to safeguard consumers, strengthen trust, and improve fraud and loss reporting for richer insights.

## The financial sector is taking a multi-layered approach:

- Deploying advanced technologies to help stop scams before they happen
- Investing in public-private partnerships
- Empowering consumers through education, because informed individuals are the first line of defense

## A Call to Collective Action

No single entity can solve this challenge alone. It is critical to double down on cross-sector collaboration both regionally and globally. Together, we can outpace the threat, restore trust, and ensure that the digital economy works for everyone.

A photograph of a man with a beard and a black cap worn backwards, sitting at a desk and talking on a mobile phone. He has a concerned expression and is holding the phone with both hands near his face. He has tattoos on his left arm. The background is blurred, showing an office environment.

# Scam Impact

What impact do scams have on victims' lives, stress and wellbeing?



Globally, the impact of scams is both financial and emotional, and over a third say they are **more vigilant of scams** as a result of their experience

58% At least one Emotional impact

36% More vigilant of scams

- 25% More distrustful of digital tools and platforms
- 17% Drop in confidence and second guessing myself
- 14% Heightened tension and stress in family unit

15% At least one Relationship impact

- 11% Blaming the victim for being careless
- 5% Break down relationships (divorce, fewer friends, etc.)

37% At least one Financial impact

- 14% Reduce normal spending behaviour
- 9% Reduced access to credit
- 8% Unable to pay for basic essentials (rent, utilities, groceries, etc.)
- 8% Take on additional debt or loans
- 7% Relatives and friends required to step in financially to support
- 7% Making additional costs (e.g., legal support, counselling)
- 6% Affect impact life milestones (buy a home, education, etc.)
- 4% Having to sell assets (car, house, etc.)

22% N/A: The scam(s) had no impact on me or my family

Q18. How has the scam(s) impacted you and your family? Base: All respondents who have been scammed (26817), North America (2996), South America (1435), Europe (9419), Africa (2778), Middle East (1535), Asia (7187), Oceania (1467)



# Scams tend to take a greater toll – emotionally, financially and socially – on lower GDP countries than on their more affluent peers

Impact of scams on victim and family – markets over-indexing on each type of impact

**58%** At least one Emotional impact

Argentina Poland   
 Brazil Saudi Arabia   
 Egypt South Africa   
 Indonesia Thailand   
 Kenya United Arab Emirates   
 Malaysia Vietnam   
 Mexico   
 Nigeria   
 Philippines



**15%** At least one Relationship impact

Argentina Mexico   
 Brazil Nigeria   
 China Saudi Arabia   
 Egypt South Korea   
 India United Arab Emirates   
 Kenya Vietnam



**37%** At least one Financial impact

Egypt South Africa   
 India South Korea   
 Japan Taiwan   
 Kenya United Arab Emirates   
 Malaysia   
 Nigeria   
 Pakistan   
 Philippines   
 Saudi Arabia



**22%** N/A: The scam(s) had no impact on me or my family

Australia New Zealand   
 Austria Singapore   
 Canada Sweden   
 France Switzerland   
 Hong Kong United Kingdom   
 Netherlands United States of America





# The majority of those affected by scams found the experience to be stressful

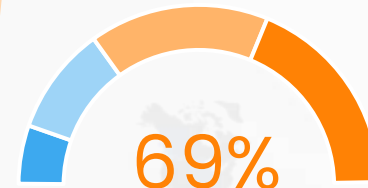
Impact of being scammed on stress

69%

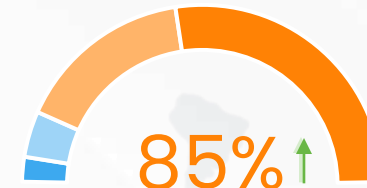
Found the scam experience very (35%) or somewhat (33%) stressful

Not stressful

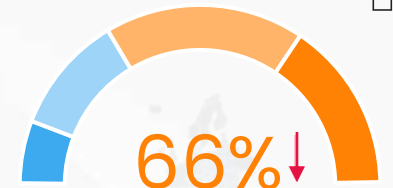
Stressful



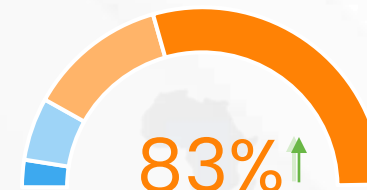
North America



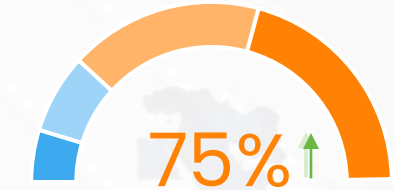
South America



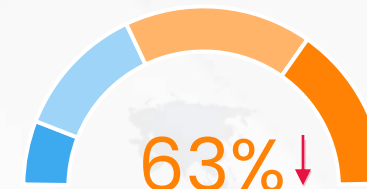
Europe



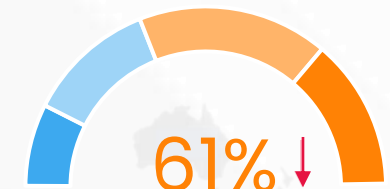
Africa



Middle East



Asia



Oceania

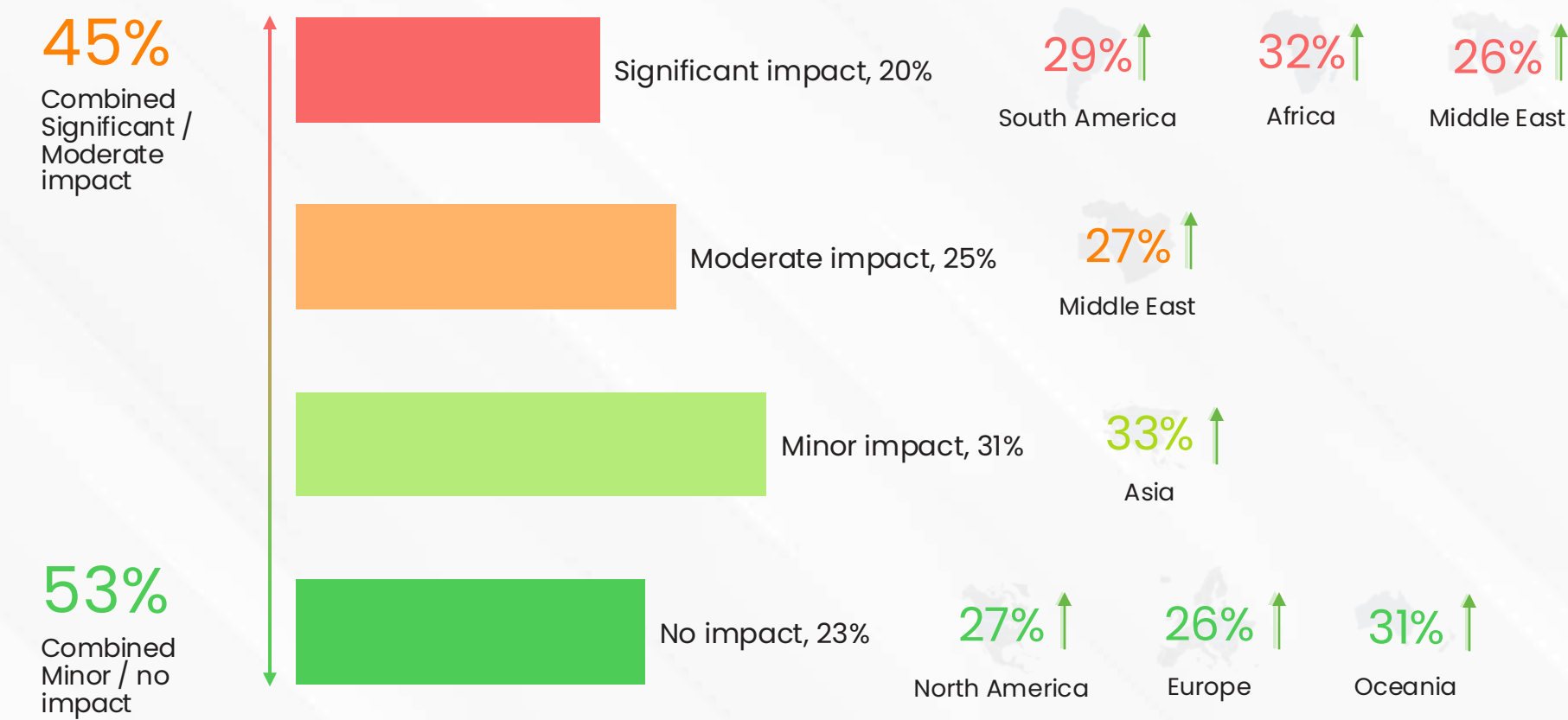
**Particularly those in South America, Africa & the Middle East**





# Regions experiencing higher levels of stress were also more likely to report that scams had a significant impact on their mental wellbeing

Impact of being scammed on wellbeing





# Scams, stress and mental health are intrinsically linked

## Scam impact summary:

Globally, the impact of scams is both financial and emotional. While over a third of victims say they have become more vigilant as a result, around a quarter now distrust digital tools and platforms. Worryingly, some victims report a loss of confidence, often second-guessing themselves. Others are becoming more cautious in their spending, struggling to access credit, or unable to afford essentials.

Scams tend to have a deeper impact in lower-GDP countries, where the emotional, financial, and social toll is often greater. In these regions, the majority of scam victims report emotional distress, while in high-GDP countries, one in five victims say the scam had no impact at all.

Despite these regional differences, most scam victims around the world experience stress, with South America and Africa particularly affected. In areas where stress levels are higher, scams are also more likely to significantly impact mental wellbeing, a pattern seen most clearly in South America, Africa, and the Middle East.

# No One Is Safe: Why Fighting Scams Requires a United Front



**Jericho Konrad**

ENTERPRISE FRAUD  
RISK DIVISION HEAD



## About RCBC

Rizal Commercial Banking Corporation (RCBC) is among the largest private domestic banks in the country in terms of assets and has a network of 459 branches and 1,448 ATMs (as of December 2022). With 60 years of long-term partnerships, RCBC has been a pillar of the banking industry, providing a wide range of financial services to its customers through its retail and investment bank, microfinance unit, foreign exchange brokerage house, leasing company and overseas remittance tie-ups. We continue to innovate and shape the future of our communities, families, and generations to come. At RCBC, we are more than just a Bank, we are proud to be Partners Through Generations.

## Scams Target Everyone

One thing that has become clear is that scammers no longer target specific demographics like they once did. The rise of social media and digital transactions means that everyone, from young digital natives to older individuals, is a potential target. Scams are now highly personalized and sophisticated, using a variety of platforms to deceive victims. This shift requires a new approach to public awareness, one that focuses on recognizing the tactics used by scammers rather than the types of people they're after.

## The Role of AFASA

A new policy that offers hope for the future is the Anti-Financial Account Scamming Act (AFASA). This law is an important step because it criminalizes key aspects of scamming, such as money muling and social engineering, and requires banks and other financial institutions to take stronger preventive measures. It allows them to temporarily hold funds from suspicious transactions and provides a legal basis to prosecute those who enable scams, for example by lending out their bank accounts. By doing so, it creates a clearer framework for financial institutions to act earlier and more decisively against fraud.

## The Need for a Unified Response

The biggest challenge in fighting scams remains the lack of a mature "whole-of-nation" approach. While the Anti-Financial Account Scamming Act (AFASA) is a significant step forward, mandating a coordinated verification process among financial institutions, this cooperation is still largely contained within the banking sector. The law creates a solid foundation for banks to share information and work together to trace funds, but the scam problem extends far beyond the financial system. Scammers leverage telecommunications providers, social media platforms, and other digital services. This fragmentation allows criminals to exploit gaps in jurisdiction and communication between different sectors.

To truly address this, there needs to be a more unified, centralized body with the authority to coordinate anti-scamming efforts across government, law enforcement, and the private sector. This would ensure a seamless flow of information, faster response times, and a comprehensive strategy to combat these evolving threats. A unified approach would not only strengthen the role of financial institutions but also hold telecommunications and social media companies accountable for their role in enabling scams.



# Prevalence of scam encounters

How frequently are scams encountered? And on what platforms?



## Scam exposure is most common in Oceania, South America and Africa

Prevalence encountering a scam in the last 12 months

**70%**  
of adults globally  
have been exposed  
to a scam in the  
last 12 months

76% ↑

North  
America

81% ↑

South  
America

66% ↓

Europe

81% ↑

Africa

68% ↓

Middle East

67% ↓

Asia

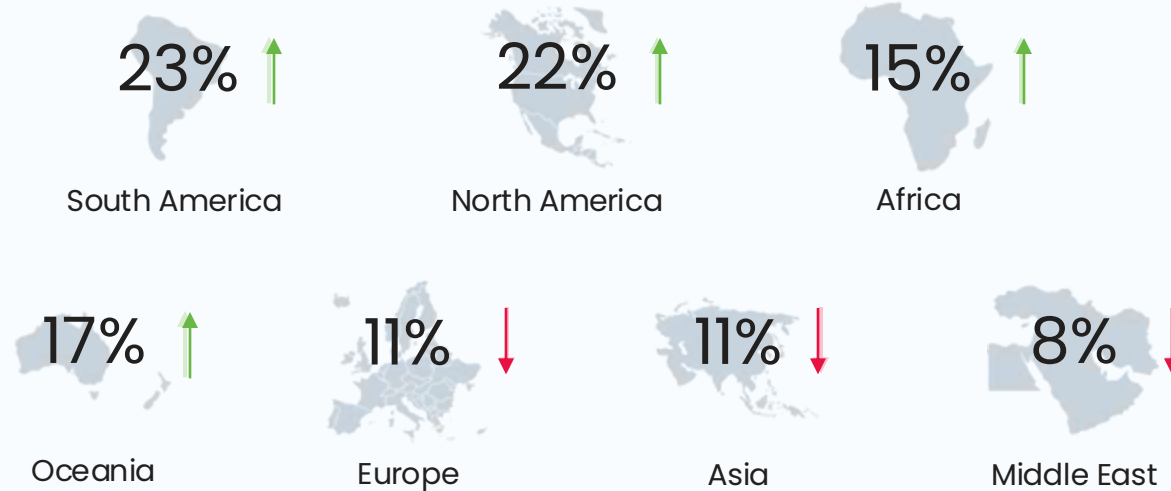
82% ↑

Oceania



# 13% encounter a scam at least once a day

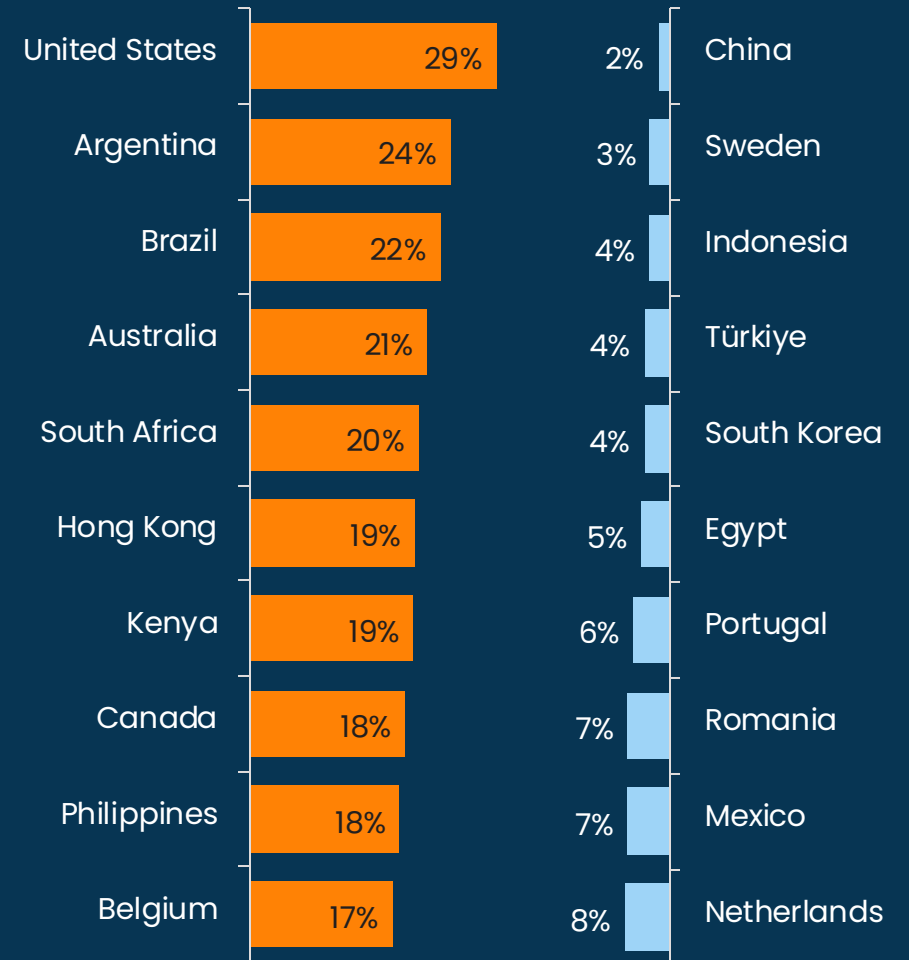
Prevalence of daily scam encounters



**This rises to nearly a quarter in South and North America. Meanwhile daily exposure to scams is less common in Europe, Asia and the Middle East**

**Top 10 countries**  
(most likely to encounter scams on a daily basis)

**Bottom 10 countries**  
(least likely to encounter scams on a daily basis)

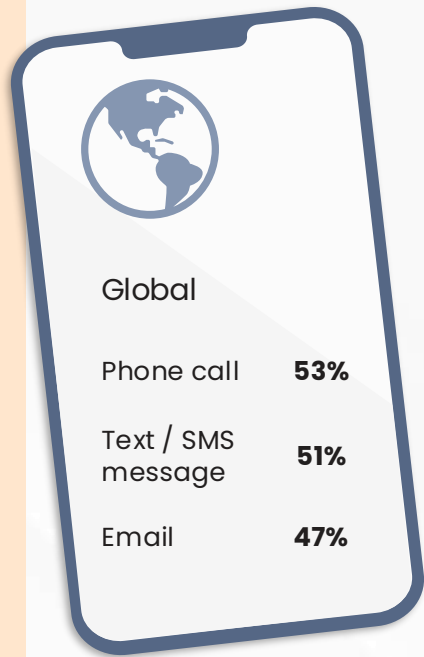




# The most common communication channels used by fraudsters

Globally are **phone calls, text messages and email**

Top three most common scammer communication channels globally and by market



## North America

Phone call	58%
Text / SMS message	55%
Email	53%



## South America

Phone call	65%
Instant messaging app	52%
Email	51%



## Europe

Email	56%
Phone call	51%
Text / SMS message	49%



## Africa

Text / SMS message	57%
Instant messaging app	50%
Social media	50%



## Middle East

Phone call	44%
Text / SMS message	41%
Social media	40%



## Asia

Phone call	57%
Text / SMS message	53%
Instant messaging app	43%



## Oceania

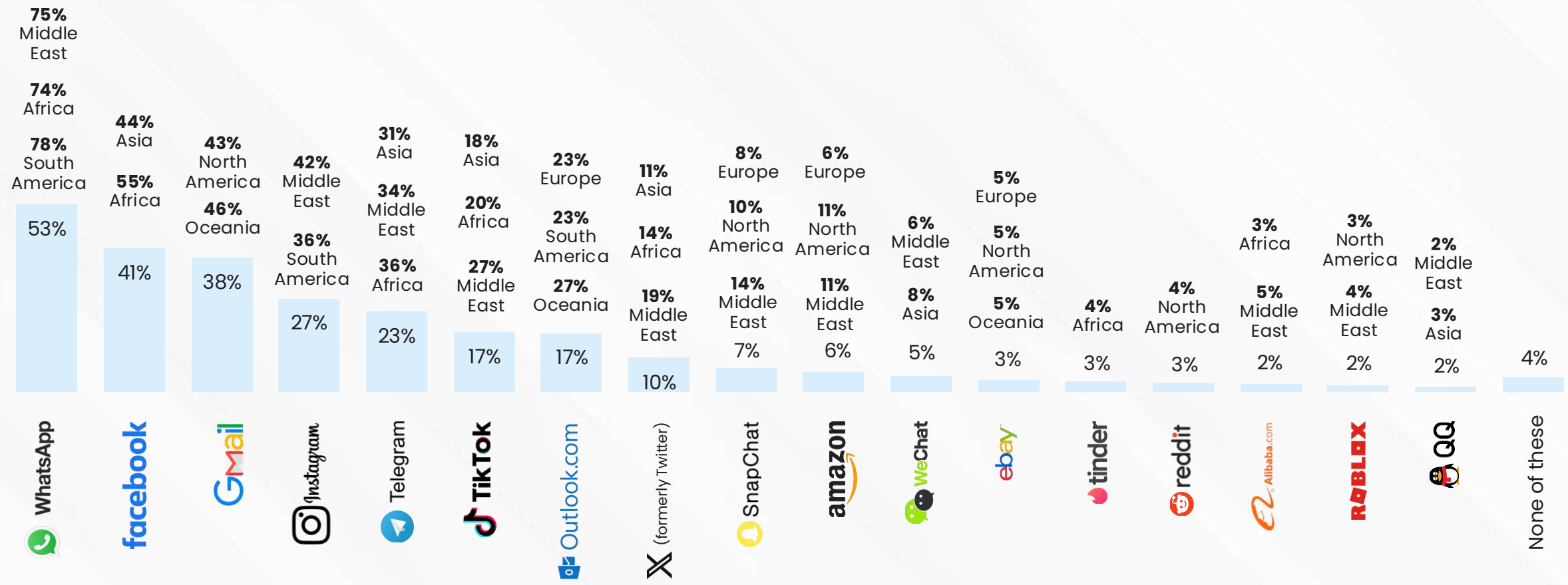
Email	66%
Text / SMS message	59%
Phone call	46%





# The most common brands that are misused by scammers are WhatsApp, Facebook and Gmail

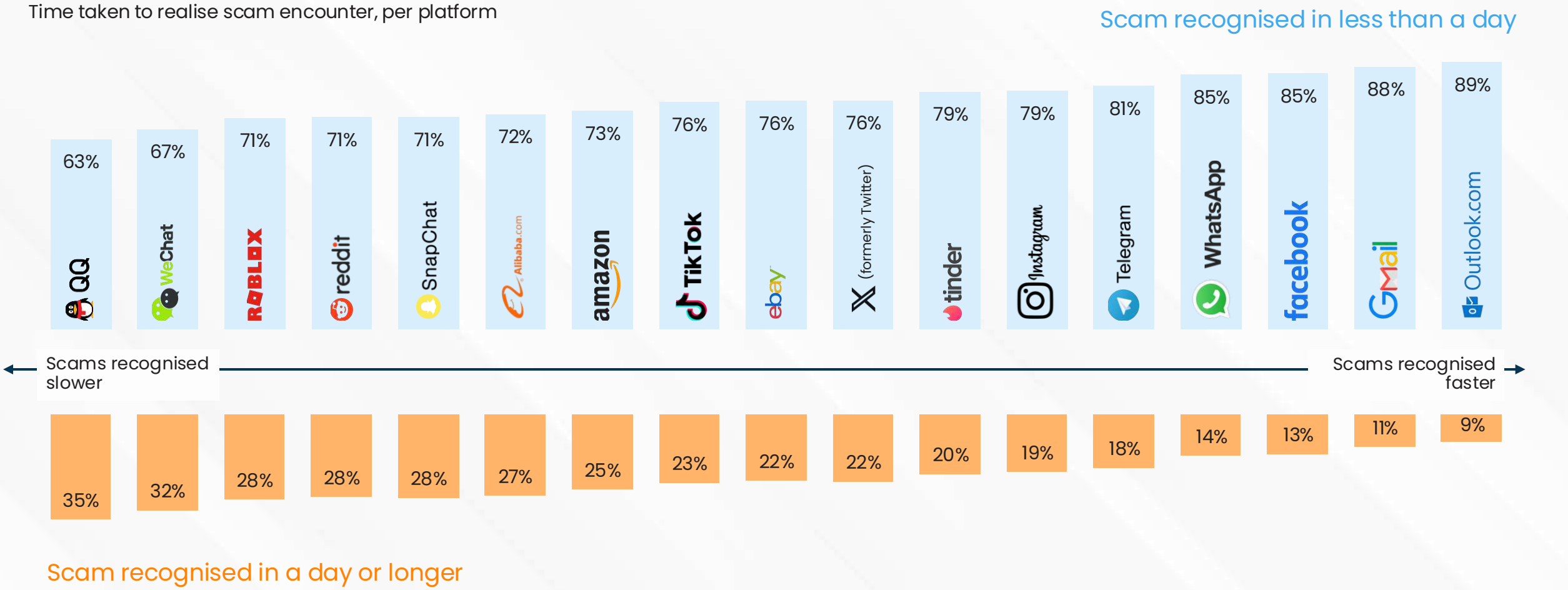
Online platforms used by scammers in last 12 months globally





# Scams tend to be recognised more slowly on smaller platforms such as QQ, WeChat, Roblox and Reddit

Time taken to realise scam encounter, per platform

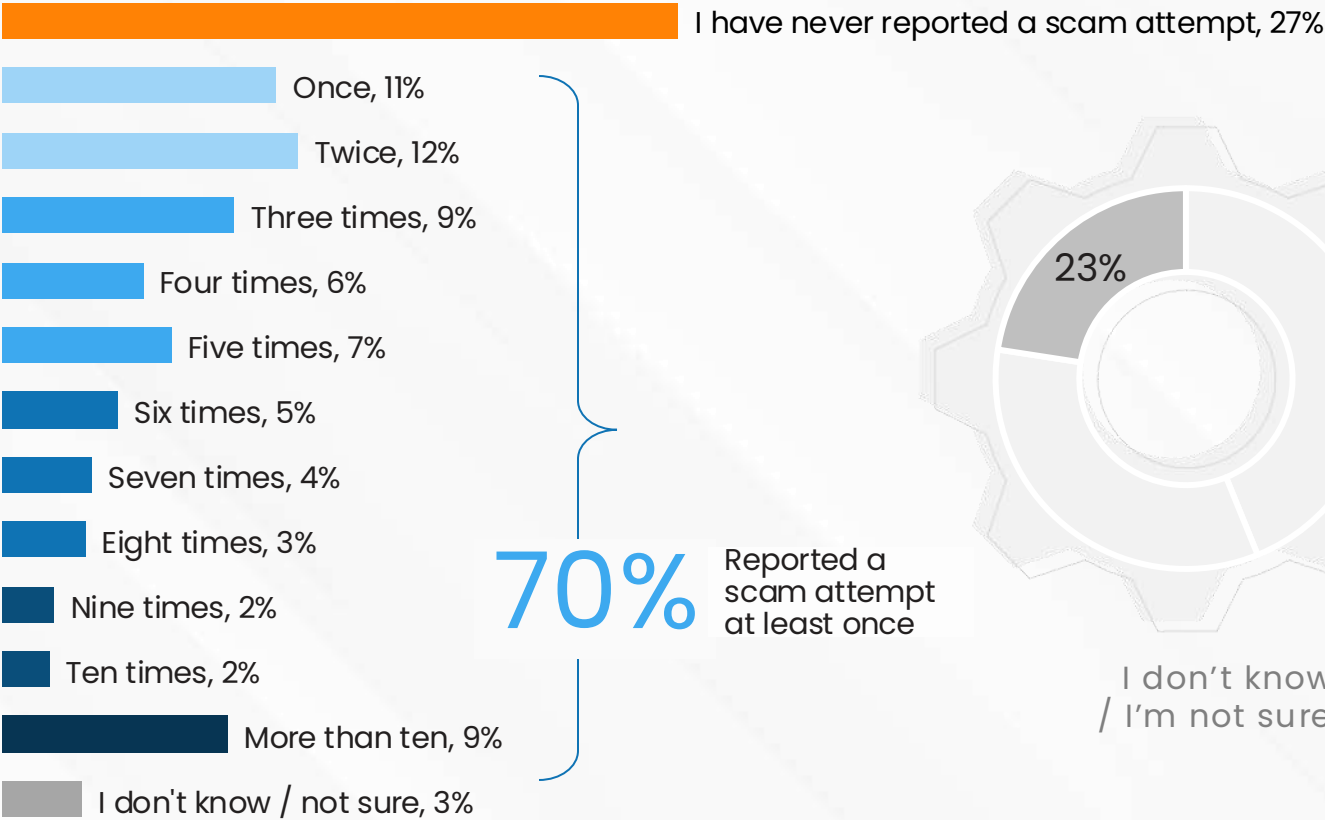


Q11. When a scammer approached you on , how long did it take you to realise they were trying to scam you? Base: All those Globally who have been contacted by a scammer on an online platform (26038)

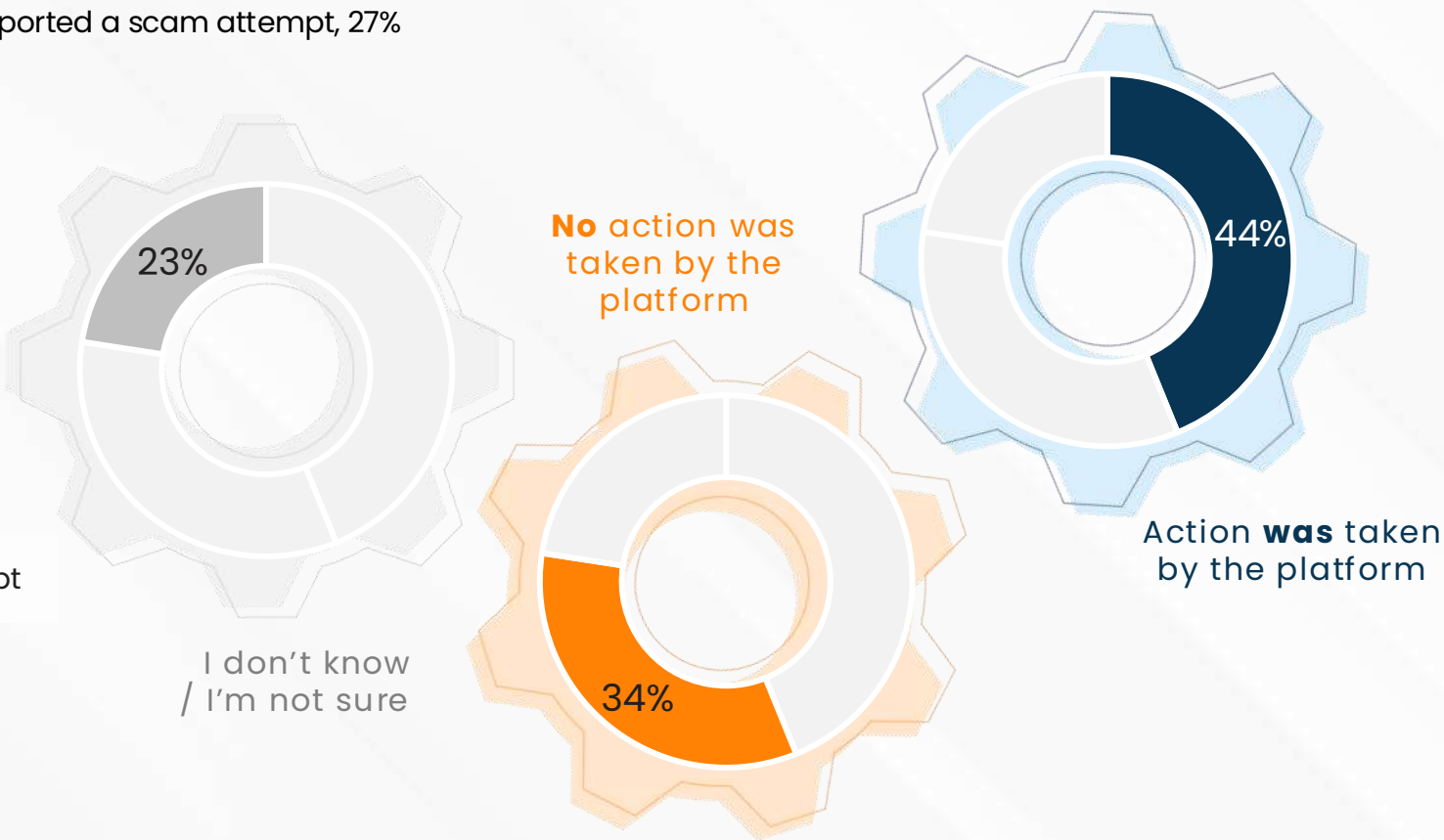


# Seven in ten of those encountering a scam have reported it **at least once**. **However**, a third say the platform took **no action** when they did so

Frequency of reporting a scam encounter in the last 12 months



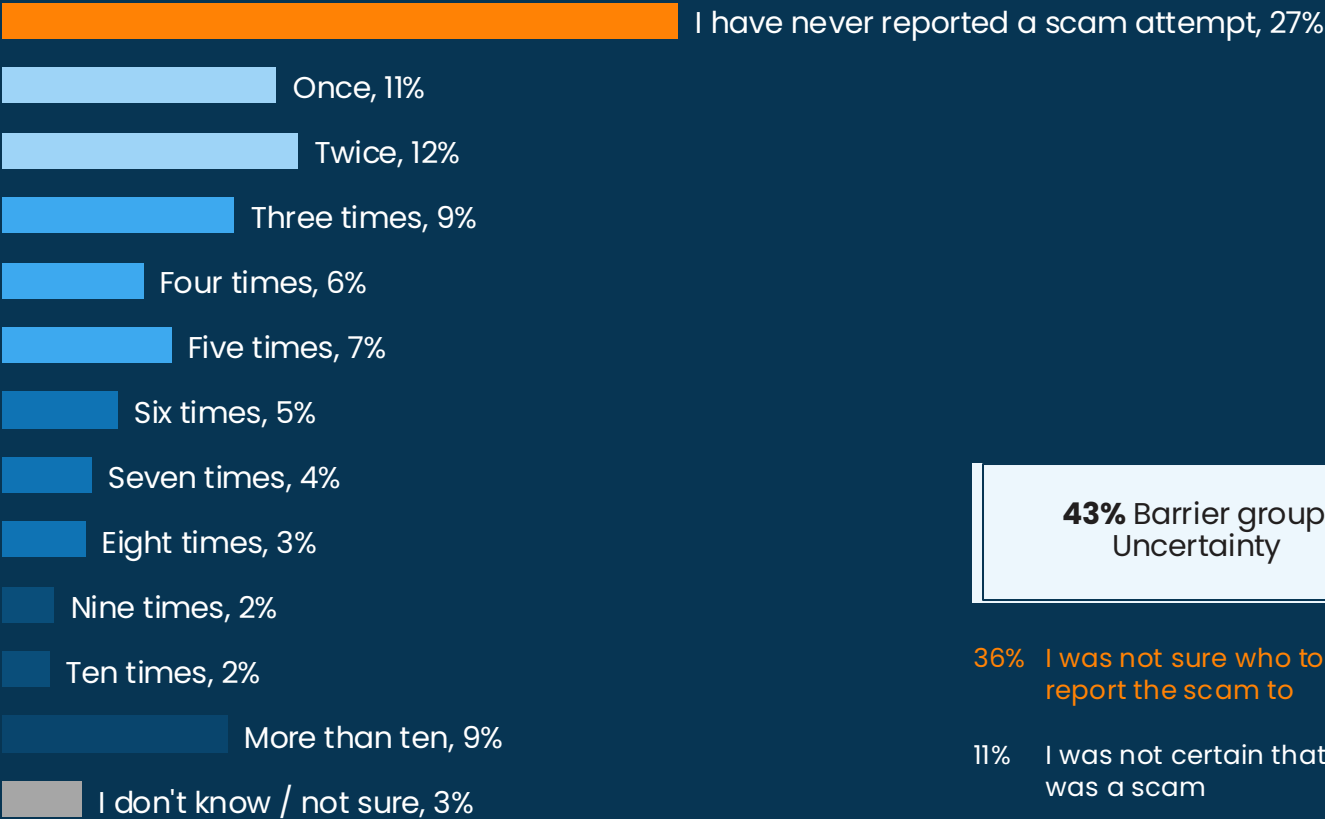
Outcome of reporting scam encounter to platform / service provider



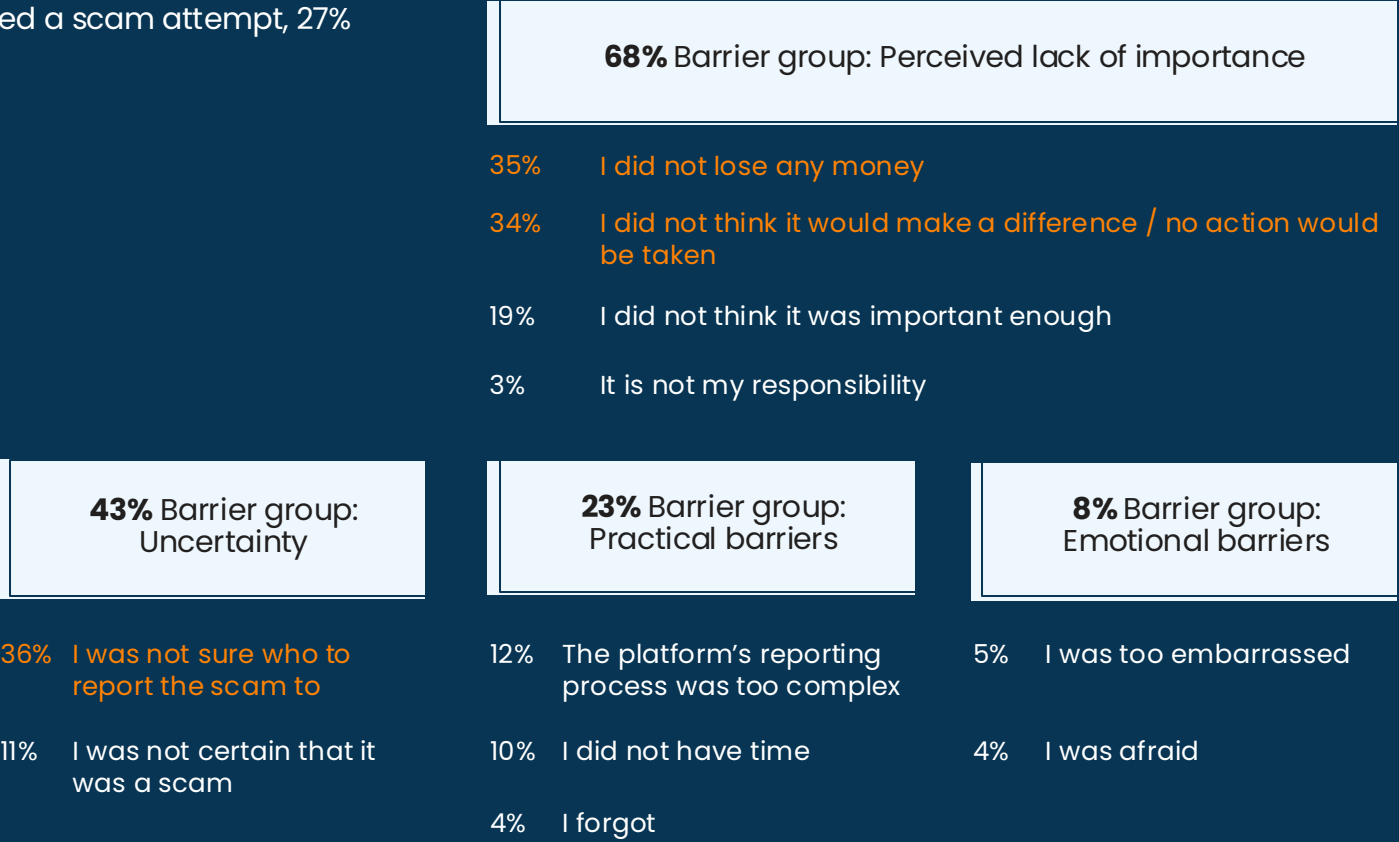


# Lack of action is one of the main reasons scam encounters go unreported, with uncertainty about who to report to being the main barrier

Frequency of reporting a scam encounter in the last 12 months



Barriers to reporting scam encounters





# Scam encounters have become part of everyday life.

## Prevalence of Scam encounters summary:

The majority of adults globally have been exposed to a scam in the past 12 months, with the highest levels of exposure in regions where scam reports are most common, particularly South America and Africa. Alarming, around one in ten people experience scam attempts on a daily basis. The USA, Argentina, and Brazil are the top three countries where daily scam encounters are most frequent.

The most common methods used to target consumers are phone calls, text messages, and emails, underlining the invasive nature of these scams. Phone scams are especially prevalent in South America, while Oceania reports the highest number of email-based scams.

WhatsApp, Facebook, and Gmail are the top global platforms where consumers are most often targeted. However, scams appear to go unnoticed for longer on smaller platforms such as QQ, WeChat, Roblox, and Reddit.

As with scam victims, the majority of those targeted have reported the scam at least once. Yet worryingly, a third say the platform took no action, a response that mirrors the experience of many actual victims.

# Trust is the Criminal's Currency, We Need to Break it Before it Begins



**Paul Benda**

EXECUTIVE VICE PRESIDENT – RISK,  
FRAUD AND CYBERSECURITY



American  
Bankers  
Association®

## About the American Bankers Association

American Bankers Association is a banking trade association of community, regional, and money center banks, holding companies, savings associations, trust companies, and savings banks. American Bankers Association provides training and education programs, information products, professional certifications, and technical services to its members. The company was founded in 1875 and is headquartered in Washington, District of Columbia.

One of the most important realizations about scams is how effectively criminals manipulate their victims to gain *trust* and bypass even the most vigilant defenses. We tell customers to only send money to people they know and trust but by the time a victim is ready to make a payment, they often feel certain they know and trust the criminal they're talking to—whether through convincing social engineering, spoofed caller IDs, or fraudulent social-media profiles. An ounce of prevention is worth a pound of cure and combating scams requires shifting our focus to earlier in the scam lifecycle—toward stopping that digital authentication through faked digital credentials.

Addressing scams requires a **whole-of-ecosystem response** that brings together financial institutions, telecom providers, social-media platforms, technology companies, government, and law enforcement. Each sector plays a role, but when efforts remain siloed, criminals exploit the gaps. The countries that have had success have a **coherent strategy focused on prevention and a shared responsibility** across all players in the scam lifecycle, built with government support, cross-sector collaboration, and robust mechanisms for information-sharing. Only with a coordinated approach can that trust be broken before its begun or that payment stopped before its made and the public better protected.

A photograph of an elderly couple in a living room. The woman is seated in a light-colored armchair, looking at a smartphone. The man is standing next to her, leaning over and looking at the phone. The room has large windows in the background and a coffee table with a tissue box and a decorative centerpiece in the foreground.

# Scam Prevention

What self-prevention tactics do consumers use to identify scams?  
How are public and commercial organisations' seen in their responsibility and performance in preventing and resolving scams?

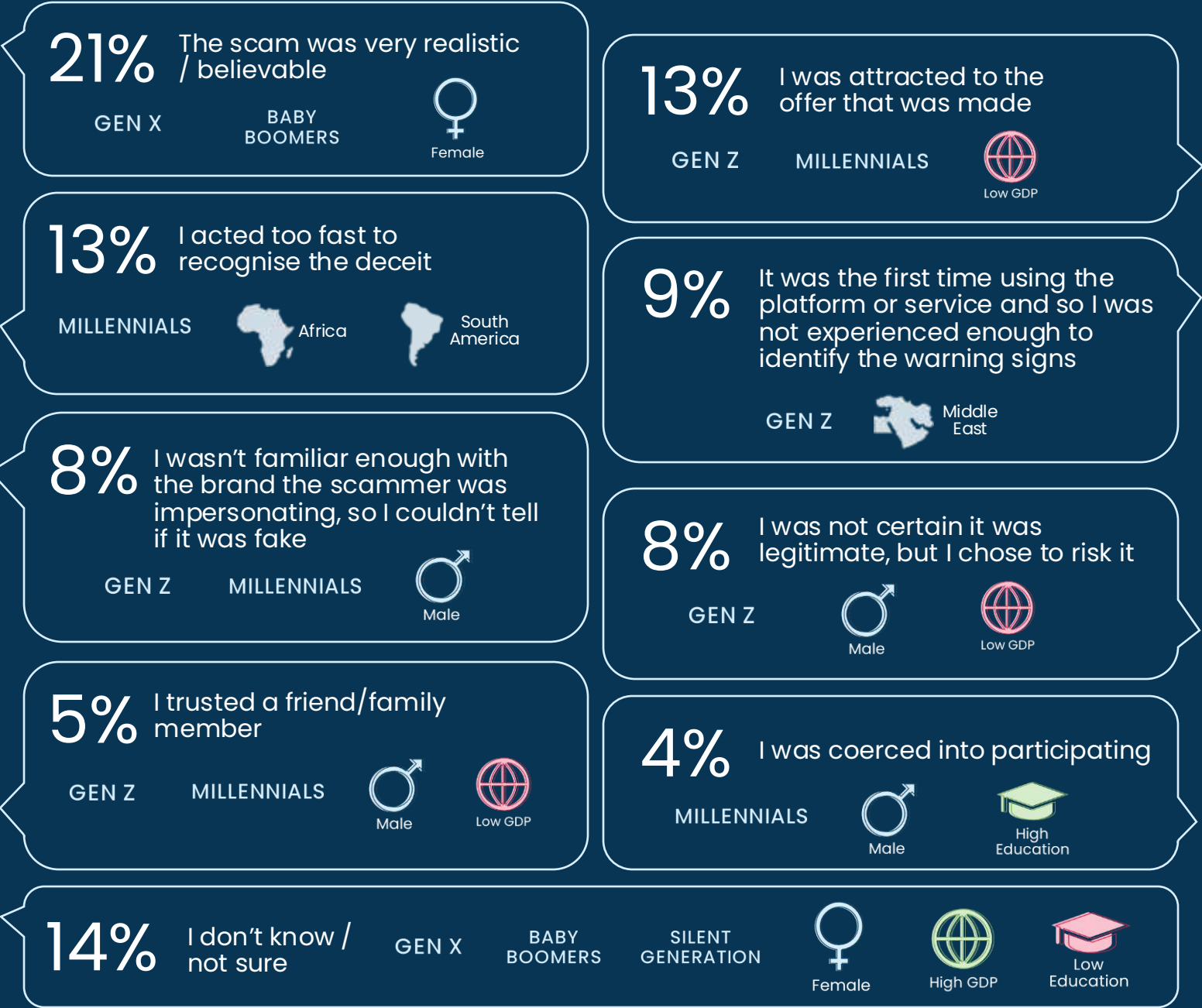




# The believability of the scam is the main reason why victims globally think they were scammed, particularly for the older generation

Reasons why scams experienced

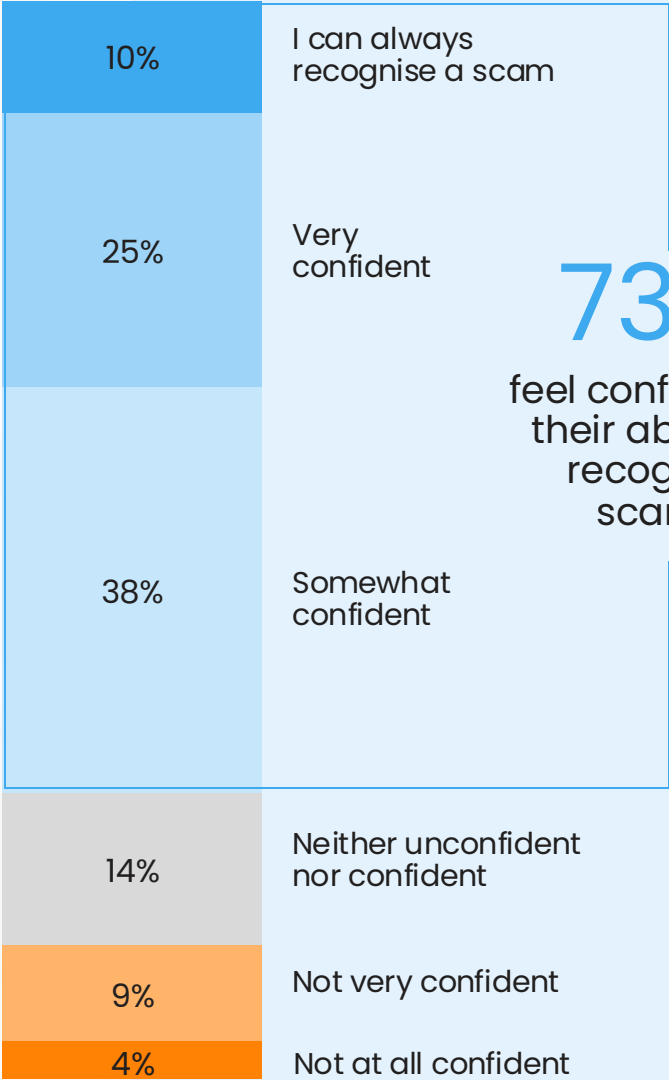
Q19. Why do you think you were scammed? Select the main reason.  
Base: All respondents Globally who have been scammed (26817)  
North America (2996), South America (1435), Europe (9416), Africa (2778), Middle East (1535), Asia (7187), Oceania (1467)



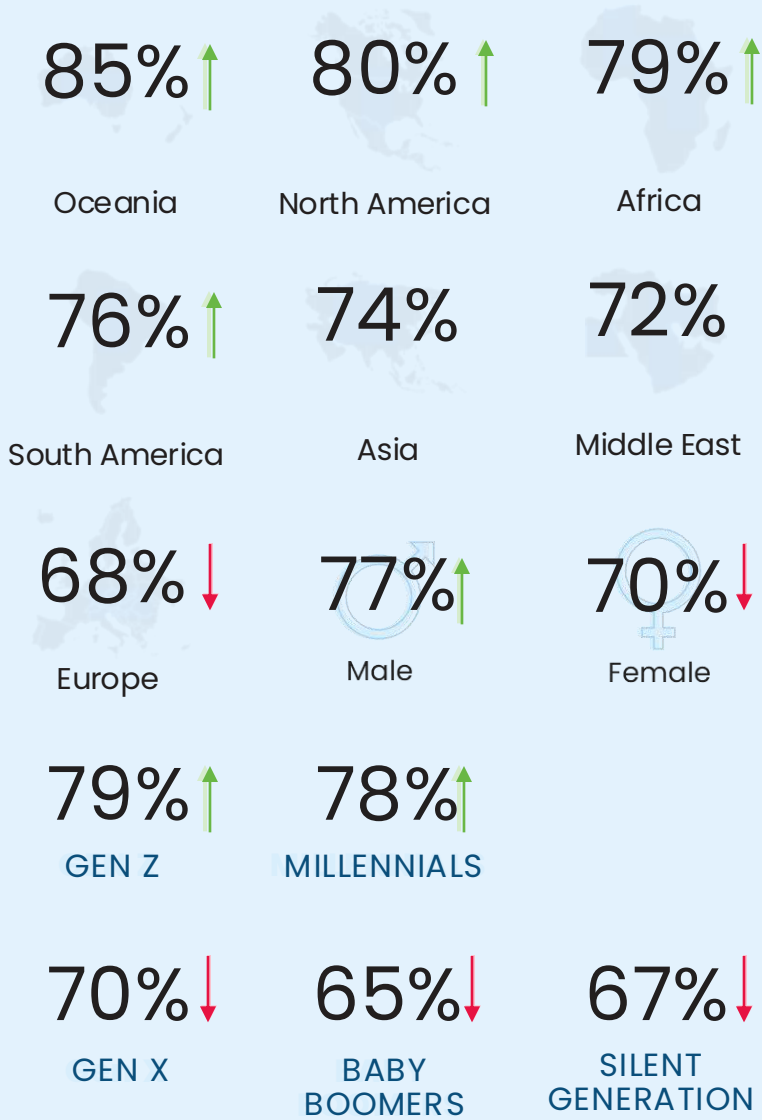


**Whilst the majority feel confident in recognising scams, older adults tend to have less confidence in their ability**

Confidence in recognising a scam



**73%**  
feel confident in their ability to recognise scams

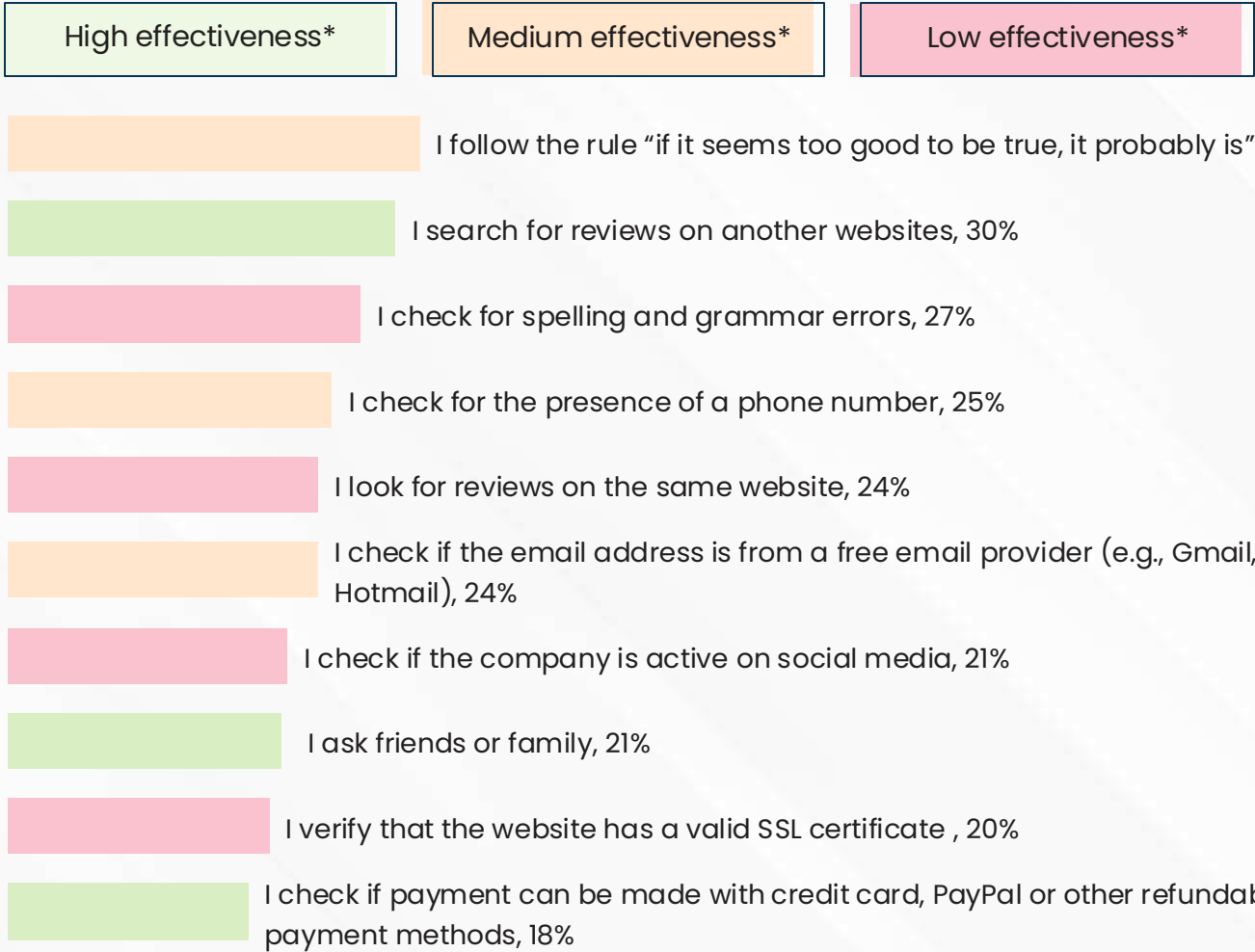




93%

of adults globally take at least one step to verify whether an offer is legitimate. However, many rely on methods that are often **less effective**

Steps taken to check legitimacy of offer – top 10

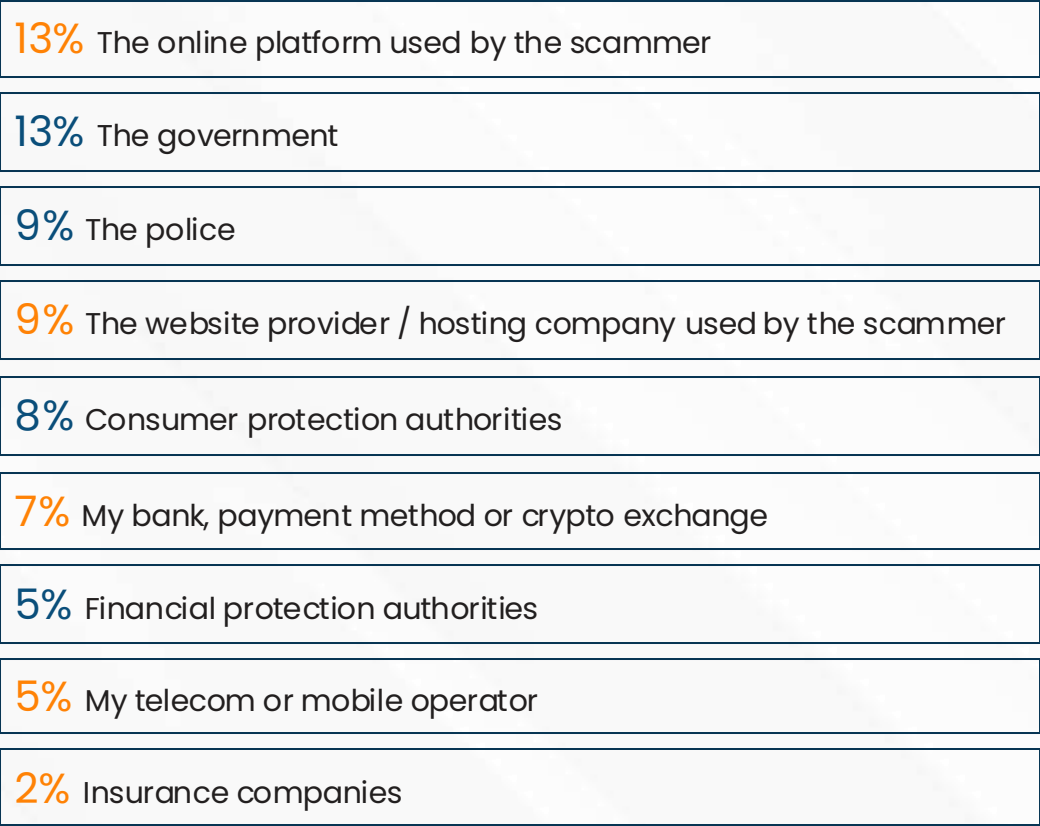
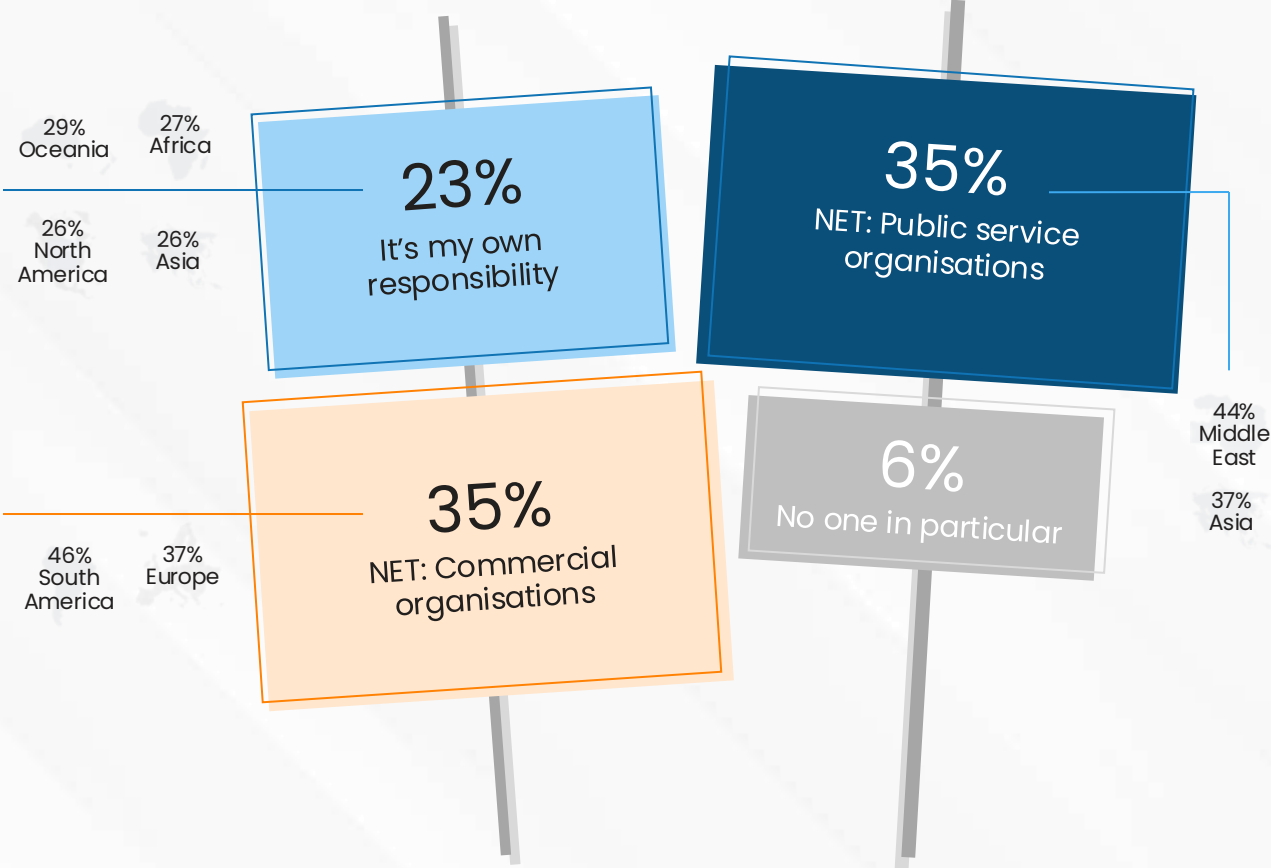


Q20. What steps do you take to check if an offer is real or a scam? Base: All respondents Globally (46000), North America (4500), South America (2000), Europe (17500), Africa (4000), Middle East (3000), Asia (13000), Oceania (2000) \*Effectiveness groupings provided by GASA



# Just over a third point to public or commercial bodies to keep people safe from scammer, whilst just under a quarter feel personally responsible

Responsibility for keeping people safe from scammers ranking:



Most responsible ↑  
↓ Least responsible



# Whilst these organisations are generally seen as adequate in scam education & reporting, there is room for improvement across the board

Consumer rating on aspects of pre & post scam support – NET: Good

	The government	The police	Consumer protection authorities	Financial protection authorities	The online platform used by the scammer	The web provider/ hosting company used	My bank, payment method or crypto exchange	My telecom or mobile operator	Insurance companies
Responsibility ranking	2 <sup>nd</sup>	3 <sup>rd</sup>	5 <sup>th</sup>	7 <sup>th</sup>	1 <sup>st</sup>	4 <sup>th</sup>	6 <sup>th</sup>	8 <sup>th</sup>	9 <sup>th</sup>
Scam education & awareness	30%	44%	41%	41%	31%	33%	48%	38%	53%
Scam blocking / payment prevention	27%	42%	37%	40%	30%	33%	48%	37%	49%
Ease of scam reporting	30%	46%	41%	40%	36%	36%	50%	37%	51%
Victim support / helpdesk	27%	44%	37%	36%	28%	30%	44%	33%	50%
Scammer investigation / arrest	29%	44%	34%	37%	26%	30%	41%	33%	49%
Reimbursement / compensation	23%	35%	31%	33%	25%	28%	43%	31%	48%
Global ranking across all aspects	9 <sup>th</sup>	3 <sup>rd</sup>	5 <sup>th</sup>	4 <sup>th</sup>	8 <sup>th</sup>	7 <sup>th</sup>	2 <sup>nd</sup>	6 <sup>th</sup>	1 <sup>st</sup>

# Protecting Consumers from Online Scams



**Abigail Bishop**

HEAD OF EXTERNAL RELATIONS



## About Amazon

Amazon is guided by a mission to be the world's most customer-focused company. It is also guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Amazon strives to be Earth's Most Customer-Centric Company, Earth's Best Employer, and Earth's Safest Place to Work. Customer reviews, 1-Click shopping, personalized recommendations, Prime, Fulfillment by Amazon, AWS, Kindle Direct Publishing, Kindle, Career Choice, Fire tablets, Fire TV, Amazon Echo, Alexa, Just Walk Out technology, Amazon Studios, and The Climate Pledge are some of the things pioneered by Amazon. For more information, visit <https://amazon.com/about>

Scammers often attempt to misuse our brand to take advantage of people who trust us. To address this, we deploy AI-based tools to proactively detect threats while our secure communication platforms keep customers connected to us safely.

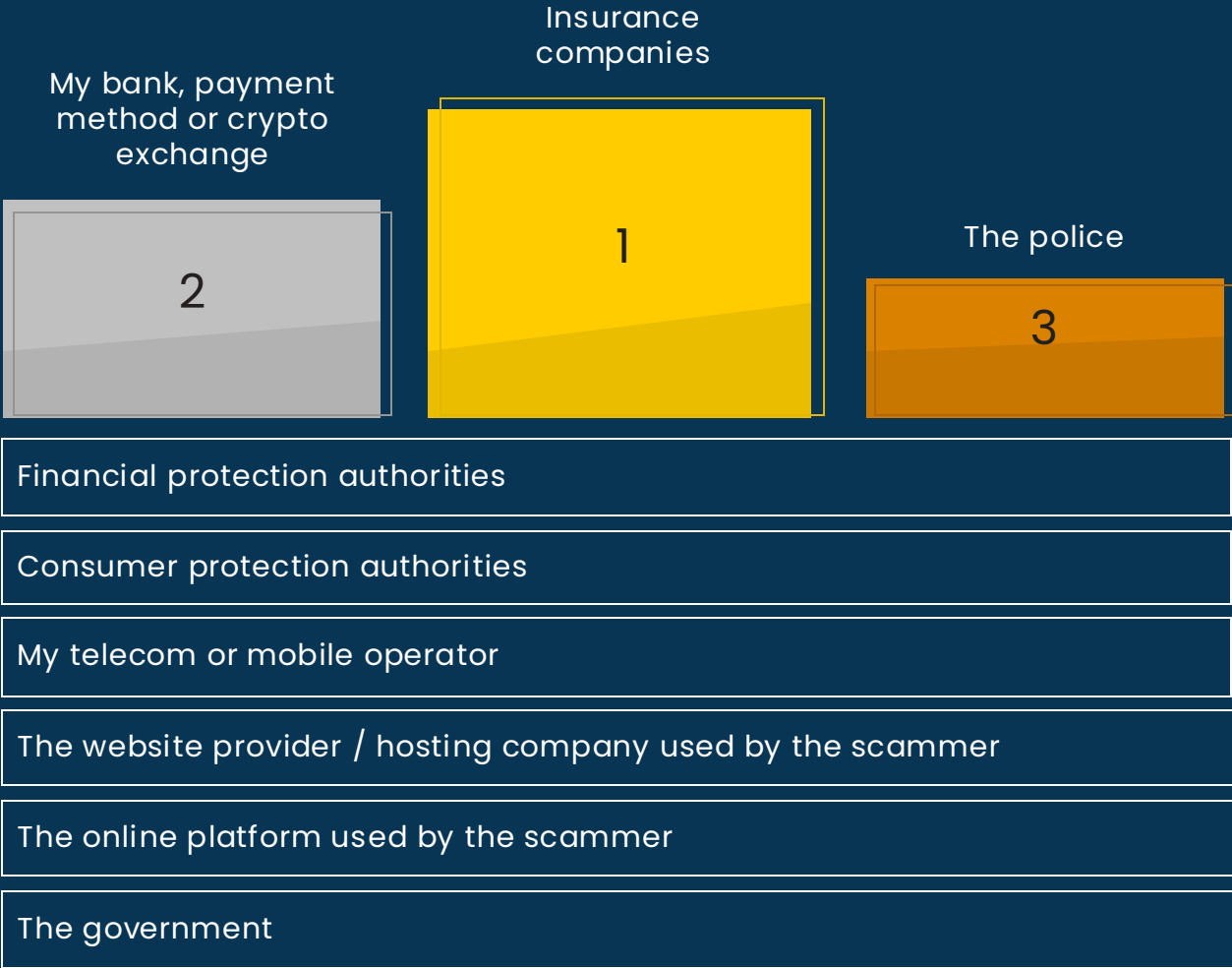
Through close collaboration with law enforcement and industry partners, we ensure bad actors are identified and held accountable. We provide self-reporting tools in more than 20 languages on our website, allowing customers to report suspicious activity directly.

These reports help our team quickly identify and stop impersonation scams, remove fraudulent sites and phone numbers, and educate consumers on prevention. In 2024, these efforts led to the takedown of over 55,000 phishing sites and 12,000 scam numbers, contributing to a 15% decrease in customers reporting being affected by bad actors impersonating us.



Overall, Insurance companies, banks & payment providers and the police are perceived to perform the strongest across all aspects of pre & post scam support globally

Performance ranking on pre & post scam support – across all aspects

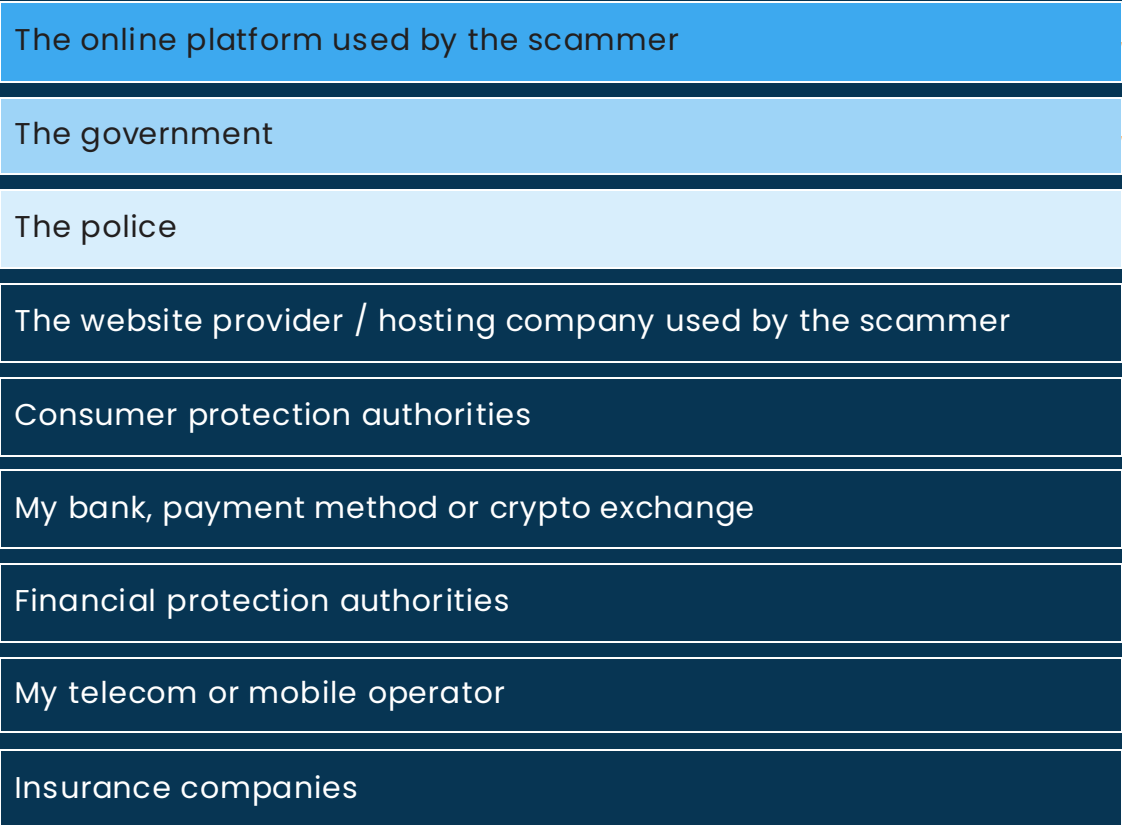






# Whilst the police perform in line with consumer expectations, the online platform used by the scammer & governments fall short

Responsibility for keeping people safe from scammers ranking:



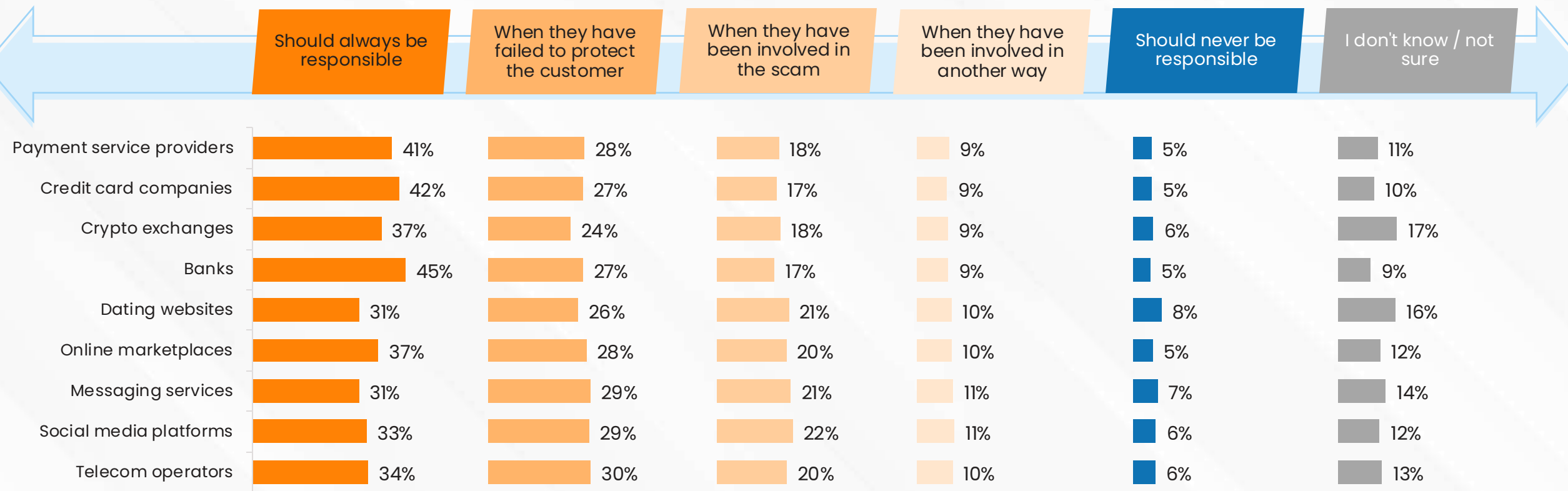
Performance ranking on preventing / resolving scams:





# Almost half of adults globally believe **Banks** should always be responsible for reimbursing those experiencing a scam

Level of expected responsibility for reimbursing scams





# Globally, full reimbursement emerged as the most supported punishment for scamming someone out of their annual income

Percentage who believe full repayment should be the maximum punishment for scamming someone out of their annual wage



Global

32%



North America

31% ↓



South America

36% ↑



Europe

35% ↑



Africa

39% ↑



Middle East

30% ↓



Asia

26% ↓



Oceania

33%



# The public feel let down by some commercial and public organisations, left to fend for themselves

## Scam prevention summary:

The main reason victims globally believe they were scammed is because the scam felt believable, particularly among older generations. Others say they acted too quickly to notice warning signs or found the opportunity too attractive to ignore. Interestingly, more than one in ten were unsure why they fell for the scam, left feeling baffled and confused.

Despite high levels of scams being successful, three in four adults globally say they're confident in their ability to recognise a scam, and one in ten claim they can always spot one. This is especially the case in North America, Oceania, and Africa. Younger adults are more likely to feel confident, yet they are often the most likely to fall victim.

Most adults take steps to verify whether something is legitimate or a scam. However, many rely on methods that are less effective, such as checking for grammatical errors, online reviews, or social media activity, highlighting a gap in education around how to stay truly safe from scammers.

Globally, consumers are divided over who should be responsible for protecting them from scams. Online platforms and governments are most commonly cited, but they're also seen as some of the worst performers when it comes to resolving issues. In contrast, insurance companies, banks, payment providers, and the police are perceived to provide the strongest support, both before and after a scam occurs. Almost half of adults globally believe that banks should always be responsible for reimbursing scam victims.

Despite all of this, a significant one in four say they feel personally responsible for protecting themselves against scams. This shows that much of the public place the burden of protection on themselves, something we might not typically expect with more traditional types of crime.



“

Protecting low-income countries from online scams and fraud is not just about safeguarding individuals—it is about preserving trust in the digital economy and society, ensuring that vulnerable communities can embrace technology with confidence, and preventing harm that deepens inequality.

**Sandra Sargent**  
**Safe Use in Digital Society Lead, The World Bank**



THE WORLD BANK

”



# GASA RECOMMENDATIONS

# GASA's ten recommendations to turn the tide on scams



**Jorij Abraham**

MANAGING  
DIRECTOR



Online scams are not just a consumer issue — they are now a major threat to digital trust, economic stability, and personal safety. As fraud networks become faster and more sophisticated, Europe needs to act decisively.

Governments often prioritize protecting critical infrastructure from cyberattacks. Yet scams targeting consumers undermine confidence in the digital economy — and criminals are evolving faster than our defences.

Through collaborative work at our global events, experts identified ten key actions to better protect consumers.



## Empowering Consumers

1. Launch unified, permanent national campaigns to raise scam awareness.
2. Establish national helplines for scam victims, accessible online and by phone.
3. Create integrated victim support systems offering financial, legal, and psychological help.

## Creating a Safer Internet

4. Build infrastructural protections with telecoms and tech providers to block scams before they reach consumers.
5. Improve fraud traceability across borders by requiring transparency from sellers, platforms, and payment providers.

## Strengthening Cooperation

6. Set up an international network of national anti-scam centres, combining law enforcement, cybersecurity, and private sector expertise.
7. Develop a global scam data-sharing hub to detect cross-border fraud in real time.
8. Make service providers responsible and liable for fraud committed through their platforms.
9. Allow preventive action: enable providers to warn, block, and take down fraudulent activities without excessive liability risk.
10. Create a global scam investigation and prosecution network to target organized fraud groups across jurisdictions.

Protecting consumers is essential to securing the digital future. The Global Anti-Scam Alliance, its membership, and the international public & private sectors must lead the way.





# ABOUT THIS REPORT



# Who are we?



The Global Anti-Scam Alliance (GASA) is a non-profit organization whose mission it is to protect consumers worldwide from scams. We realize our mission by bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, telecom operators, internet platforms and service providers, cybersecurity and commercial organizations to share insights and knowledge surrounding scams. We build networks in order to find and implement meaningful solutions.

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 world's first end-to-end financial crime prevention platform, protecting people and payments with AI-native solutions that stop fraud and financial crime. Leading financial institutions trust Feedzai to manage critical risk and compliance processes, safeguarding trillions of dollars of transactions while improving the customer experience and protecting the privacy of everyday users.

Feedzai is committed to providing its clients with the most advanced and effective solutions and expertise while driving innovation and advancing the fight against financial crime.



Opinium is an award-winning strategic insight agency that utilises robust methodologies to deliver insights with impact for organisations across the private, public and third sectors.

GASA have partnered with Opinium to lead the 2025 Global State of Scams research programme.

Contact [europe@opinium.com](mailto:europe@opinium.com) for enquiries.

# Methodology notes

## SAMPLE AND METHODOLOGY

- Sample size | 2,500 people
- Audience | Adults aged 18+ living in United States of America
- Quotas | Quotas were used throughout fieldwork to ensure the sample was nationally representative of the American adult population on age, gender and region
- Weighting | Weighting was applied on the final dataset to be nationally representative of the American adult population on age, gender and region
- Methodology | 15-minute online survey
- Translations | Whilst this report is in English, the survey was translated into the local language for each market prior to completion by respondents
- Sample source | Online research panel
- Fieldwork | 26<sup>th</sup> February – 14<sup>th</sup> March 2025

## VALUE LOST TO SCAMS CALCULATION

In this Nationally Representative survey of 2500 American adults, 558 lost money to scams.  $558 / 2500 * 267081433$  (U.S. adult population. Source: United States Census Bureau) = 59612576 (shorthand 59.6 million).  $\$1086.7 * 59612575.8456 = 64780986171.4135$  (shorthand \$64.8 billion).

## SURVEY APPROACH CHANGES

The statistical approach adopted in this year's survey represents a **different approach** compared to previous reports. While many of the questions remain unchanged, any historical comparisons should be treated with caution. More thorough data cleansing measures were also implemented throughout fieldwork. Outliers were scrutinized and, as a result, the top 2 percent of the highest amounts reported were automatically excluded as a minimum. In some countries with a higher number of extreme cases, this figure was increased to 5 percent, which in practice meant removing up to 50 respondents.

This year also provides a **more representative sample**, with quotas set on age, gender, and region. The research agency Opinium conducted the survey, addressing earlier limitations, and, results were weighted accordingly across all 42 markets surveyed.

Finally, the survey reports a **different amount** compared to last year. Unlike earlier reports that extrapolated results to the global population, this year's figure reflects only the 42 markets surveyed. This new approach will be adopted in future reports to ensure more consistent and representative results.

# Methodology notes

## FULL Q8 SCAM WORDING USED IN SURVEY

- **Investment scam:** Invested money with a person or company that deceived you about what you would receive, such as promising a guaranteed return on your investment or no risk of financial loss
- **Shopping scam:** Paid for any products or (subscription) services that you never received or that turned out to be a scam
- **Employment scam:** Paid money or given personal/financial information to get a job, employment, work-at-home position or business opportunity but were deceived about how the money would be used or what you would receive in return
- **Unexpected money scam:** Paid money or given personal/financial information to receive a prize, grant, inheritance, lottery winning, or sum of money that you were told was yours, but never received
- **Impersonation scam:** Paid money or given personal/financial information to a person who claimed to be a government official or working for a bank/lender or other company of authority
- **Charity scam:** Donated money to a charity or a charitable cause that later turned out to be fake or that you later suspected was fake
- **Romance/relationship scam:** Given money or personal/financial information to someone who pretended to be or pretended to be calling on behalf of a family member, friend, caregiver, or someone interested in you romantically, but that person was not who they claimed to be
- **Fake invoice scam:** Paid an invoice or a debt, but you found out you were being deceived, and the invoice/debt was not real or not yours
- **Blackmail or extortion scam:** Paid money or given personal/financial information because someone threatened or extorted you
- **Identity theft:** Personal information, e.g. your credit card, used without your consent OR did someone get access to a personal account(s), e.g., your bank, email, social media account, for financial gain, for example, to transfer money, take out a loan, request official documents, or buying products and/or services
- **Money recover scam:** Paid money or given personal/financial information to a company or person who promised to help me recover from a scam, but in the end deceived me.
- **Other scams:** Where you have paid money or given personal/financial information to someone who used deception in another situation not previously listed



# ABOUT THE AUTHORS



# About the authors



**Jorij Abraham**

MANAGING DIRECTOR



Jorij Abraham has been active in the Ecommerce Industry since 1997. From 2011 to 2017, he was the Research Director of Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and Managing Director of the Ecommerce Foundation.

From 2015 to 2024, Jorij was also a Professor of Ecommerce at TIO University. In 2018, Jorij took over ScamAdviser.com to help consumer due diligence efforts against online scams. He sold ScamAdviser to Gogolook in 2024 to focus on his current role as Managing Director at the Global Anti-Scam Alliance (GASA).



**Molly Maclean**

ASSOCIATE DIRECTOR



Molly Maclean is an Associate Director specialising in research for Thought Leadership.

Molly works with brands and organisations to help them use insights to raise awareness of key issues, influence decision-makers, and drive positive change.

She has over six years of experience conducting research for technology brands and organisations, particularly in the cybersecurity space.



**Metje van der Meer**

MARKETING DIRECTOR



Metje van der Meer leads global communications, brand strategy, and stakeholder engagement at the Global Anti-Scam Alliance (GASA). With over a decade of experience in B2B marketing and international outreach, she develops multi-channel campaigns and partnerships that advance GASA's mission to combat online fraud through cross-sector collaboration.

Metje plays a key role in promoting GASA's global and regional initiatives, including the Global Anti-Scam Summit (GASS) and the alliance's work across the globe. Her efforts focus on aligning public and private sector stakeholders to raise awareness and drive coordinated action against scams worldwide.

# Join GASA, the Network to Defeat a Network

## Exclusive Intelligence Sharing

Stay ahead of emerging scam trends through members-only webinars, expert-led discussion groups, and our monthly newsletter which is trusted by over 20,000 anti-scam professionals worldwide.

## Authoritative Research Access

Get insider access to our Global State of Scam reports, 30+ in-depth regional studies, and best practice database that help shape anti-scam strategies.

## High-Impact Networking

Connect with global changemakers at international summits, collaborate through local GASA chapters, and find partners through our members-only directory.

## Global Solutions

Co-create or join concrete solutions to fight scams like the Global Signal Exchange where data is shared real-time scam intelligence and Scam.Org, the anti-scam hub being developed for consumers worldwide.

**Become part of a global force against scams and help protect consumers everywhere.**

See all benefits: [gasa.org/membership](https://gasa.org/membership)

## Our Foundation Members



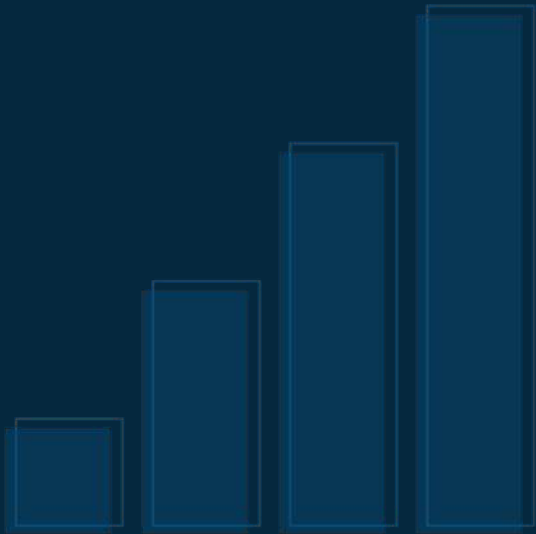
## Our Corporate Members

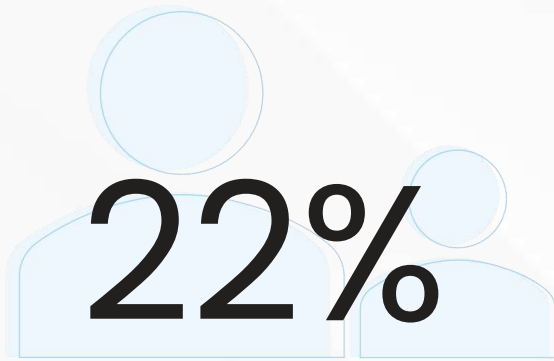






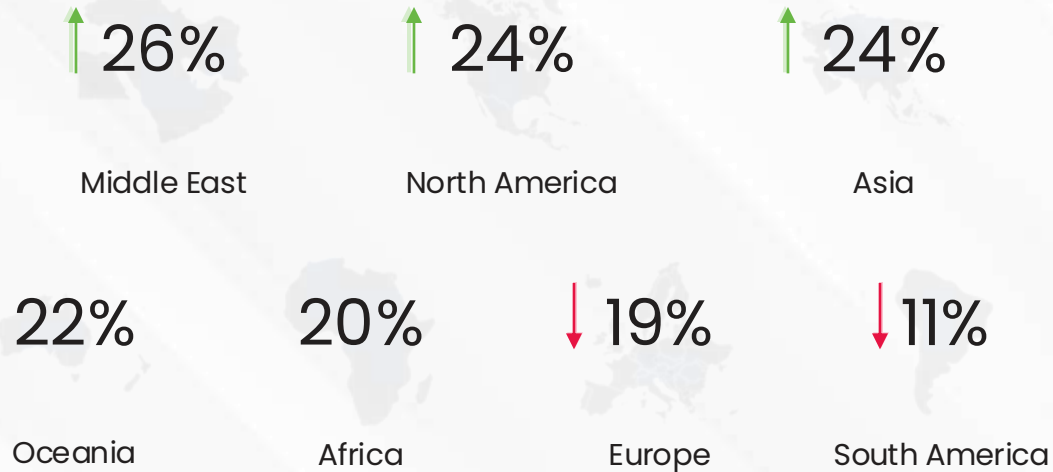
# APPENDIX



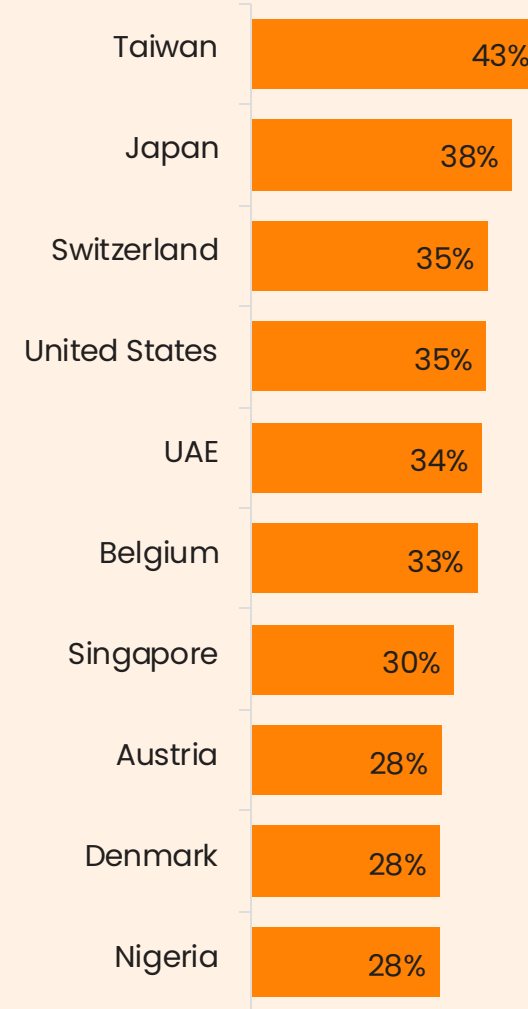


Of parents **globally** with a child aged 7-17 say at least one of their children has been scammed

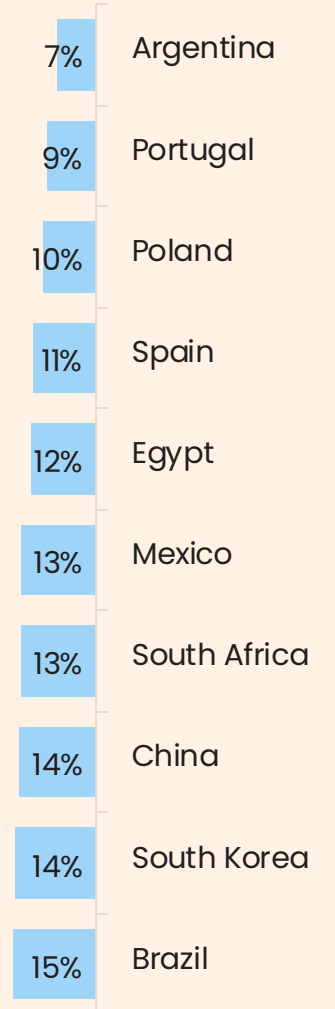
Proportion of parents reporting scam experiences amongst their children



Ten **highest** proportion of parents reporting scam experiences amongst their children



Ten **lowest** proportion of parents reporting scam experiences amongst their children





## DISCLAIMER

This report is a publication by the Global Anti-Scam Alliance (GASA) supported by Feedzai. GASA owns the copyrights for the report. Although the utmost care has been taken in the construction of this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

## COPYRIGHT

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

## Global Anti-Scam Alliance (GASA)



Oder 20 – UNIT A6311  
2491 DC The Hague  
The Netherlands



General & Press Inquiries: [partner@gasa.org](mailto:partner@gasa.org)



X (Twitter):  
[@ScamAlliance](https://twitter.com/ScamAlliance)



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