

GASA

Global Anti-Scam Alliance



Powered by Generali

State of Scams in the United States of America

2025 REPORT

INSIGHTS

LEARN MORE



The Scam Crisis Hitting Every American: 377 times per year



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.



Powered by Generali

If you haven't been targeted by a scammer this year, you're in the minority. Our reporting reveals that 70% of American adults fell victim to scams in 2025 – and the numbers are getting worse, not better.

Criminals stole \$64.8 billion from Americans in just one year, with each victim losing an average of \$1,087. But here's what's especially alarming: we're all under constant attack. The average American now encounters a scam attempt every single day – 377 times per year.

Why Scams Are Getting Smarter: What makes today's scams so dangerous isn't just their frequency – it's their sophistication. Criminals are now using artificial intelligence to create scams that would have seemed impossible just a few years ago. They can clone your voice with just 3-5 seconds of audio, create convincing deepfake videos in real-time, and impersonate anyone with frightening accuracy.

Tools like FraudGPT have essentially democratized advanced fraud techniques, meaning criminals no longer need to be tech experts to pull off convincing scams. The result? Impersonation scams will continue to grow, and they are already in the top five of scam typologies reported in this survey.

Where Scammers Find You: They're coming through the channels you use every day. Text messages lead the pack at 56% of scam attempts, followed closely by email at 55%. These aren't random attacks – scammers are strategically targeting the platforms where we're most comfortable and least suspicious.

The Hidden Costs & Following the Money: The financial losses are devastating, but they're just the beginning. Two-thirds of scam victims report significant stress, with many developing lasting anguish about digital interactions. Even worse, 12% of victims had to cut back on normal spending, creating ripple effects that hurt the broader economy.

Forget what you've heard about cryptocurrency being the scammer's payment method of choice. The reality is more troubling: they're successfully exploiting traditional channels like debit cards (30% of cases) and PayPal (25%), proving that no payment method is truly safe.

Your Next Move: This isn't just about protecting your money – it's about protecting our entire digital ecosystem. Stay informed about evolving scam tactics, verify suspicious communications, and report all fraud attempts to help protect yourself and your community.

The True Cost of Silence – And a Call to Act



Paige L. Schaffer

CHIEF EXECUTIVE OFFICER



Powered by Generali

About Iris® Powered by Generali

Iris® Powered by Generali is a B2B2C global identity and cyber protection company owned by the 190-year-old multinational insurance company, Generali, that is passionate about not just developing effective identity protection solutions but also integrating them into people's lives in a meaningful and impactful way.

Today, we partner with some of the world's most well-known brands, protecting their people how they want to be protected, no matter where they are.



Powered by Generali

At Iris® Powered by Generali, we don't just offer identity and cyber protection; we build the infrastructure that makes it work. We connect the vendors, data sources, partners, and platforms to create seamless, intuitive experiences that fit naturally into people's lives, meeting them where they already are, so that protection isn't just available, but refreshingly usable.

As a B2B partner powering identity protection behind some of the world's most recognized brands for over two decades, we've seen firsthand how quickly scams evolve – and how easy it is to underestimate the scale of the threat.

The findings in this year's *State of Scams in the United States* report make it painfully clear. A whopping 7 in 10 U.S. adults say they've been scammed in the past year. The average scam victim lost over \$1,000. And most people are encountering more than one scam a day, equating to 377 encounters per person, per year.

But recognizing the scope of the problem is only the beginning. What matters now is *what we do next*.

At Iris, we believe the path forward is rooted in accountability – for all organizations, starting with ourselves. For us, that means: No bloated feature sets that distract from real utility. Instead, end-user impact is at the core of our development work. No offloading responsibility – our partners' success is our success.

We are keenly aware that this work can't be done alone. That's why we're intentional about the partnerships we pursue – working with organizations that understand that scam prevention isn't just good business, it's a moral responsibility. Together, we aim to simplify complexity, close critical knowledge gaps, and provide protection that empowers people.

The True Cost of Silence – And a Call to Act



Paige L. Schaffer

CHIEF EXECUTIVE OFFICER



Powered by Generali

About Iris® Powered by Generali

Iris® Powered by Generali is a B2B2C global identity and cyber protection company owned by the 190-year-old multinational insurance company, Generali, that is passionate about not just developing effective identity protection solutions but also integrating them into people's lives in a meaningful and impactful way.

Today, we partner with some of the world's most well-known brands, protecting their people how they want to be protected, no matter where they are.



Powered by Generali

So, let's get to the root of the issue: This report shows that scammers are exploiting gaps in confidence, clarity, and communication.

Almost 6 in 10 of those reporting a scam in the last 12 months say that either no action was taken (29%) or they aren't sure what the outcome was (28%). Close to 40% of victims say that they were not able to recover any of their lost money when they reported the scam to the payment service, and just 44% were able to recover some of their losses. These aren't just statistics – they're warning signs that trust and support (and accountability!) are in short supply.

We've seen similar sentiments in our recent 2025 Identity & Cybersecurity Concerns (ICC) survey, where 1 in 2 fraud victims say their recovery process was difficult, and 93% reported significant stress involved with the resolution process. Institutional inaction, lack of support, difficult reporting and resolution pathways all give scammers more room to operate.

This is why all companies must take an active, ongoing role in scam education and prevention. By implementing these three things, we believe real change is within reach:

- 1. Say clearly that reporting matters.** Don't assume people know what to do. Tell them (often!).
- 2. Make reporting easy.** Provide simple, intuitive pathways to act and get support.
- 3. Invest in tools that empower your customers.** Surface proactive alerts. Provide guidance. Make education a priority, not an afterthought.

Doing so doesn't just protect your customers. It protects your brand. Scammers follow the path of least resistance. And when customers see that you're watching out for them, you don't just reduce risk, you earn trust that lasts.

This report is a wake-up call. The data is disturbing – but it also lights a path forward.

Fraud and scams are no longer just a consumer protection issue



Kate Griffin

DIRECTOR, NATIONAL TASK FORCE
ON FRAUD AND SCAM PREVENTION



About the Aspen Institute Financial Security Program

The Aspen Institute Financial Security Program's (Aspen FSP) mission is to illuminate and solve the most critical financial challenges facing American households and to make financial security for all a top national priority.



Powered by Generali

Fraud and scams are not only a consumer protection issue—they are a national security crisis. At the Aspen Institute Financial Security Program, we see how transnational criminal organizations use fraud and scams to generate billions of dollars 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's 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.

In the U.S., stakeholders must work together to elevate fraud and scam prevention as a national priority. Federal efforts remain fragmented. Agencies lack the tools to share intelligence swiftly, and victims often don't know where to turn for help. Meanwhile, private-sector organizations—many of whom are making meaningful efforts to educate and protect their customers—are too often left to fight this crisis alone.

To coordinate action among these stakeholders, we need a national strategy in the United States. That's why the Aspen Institute Financial Security Program has convened the National Task Force on Fraud and Scam Prevention. We've brought together leaders from consumer protection, technology, finance, and law enforcement to design an action plan that strengthens cross-sector coordination, recommends policy updates, and gives every American better protection and recourse when targeted.

For consumers, fraud is not just a financial blow. 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.

That's why the Task Force's strategy isn't just about crime prevention; it's about defending vulnerable populations, cutting off funds for global criminal networks, and restoring trust in our economy.

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.

www.mastercard.com

www.mastercard.com



Powered by Generali

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.

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

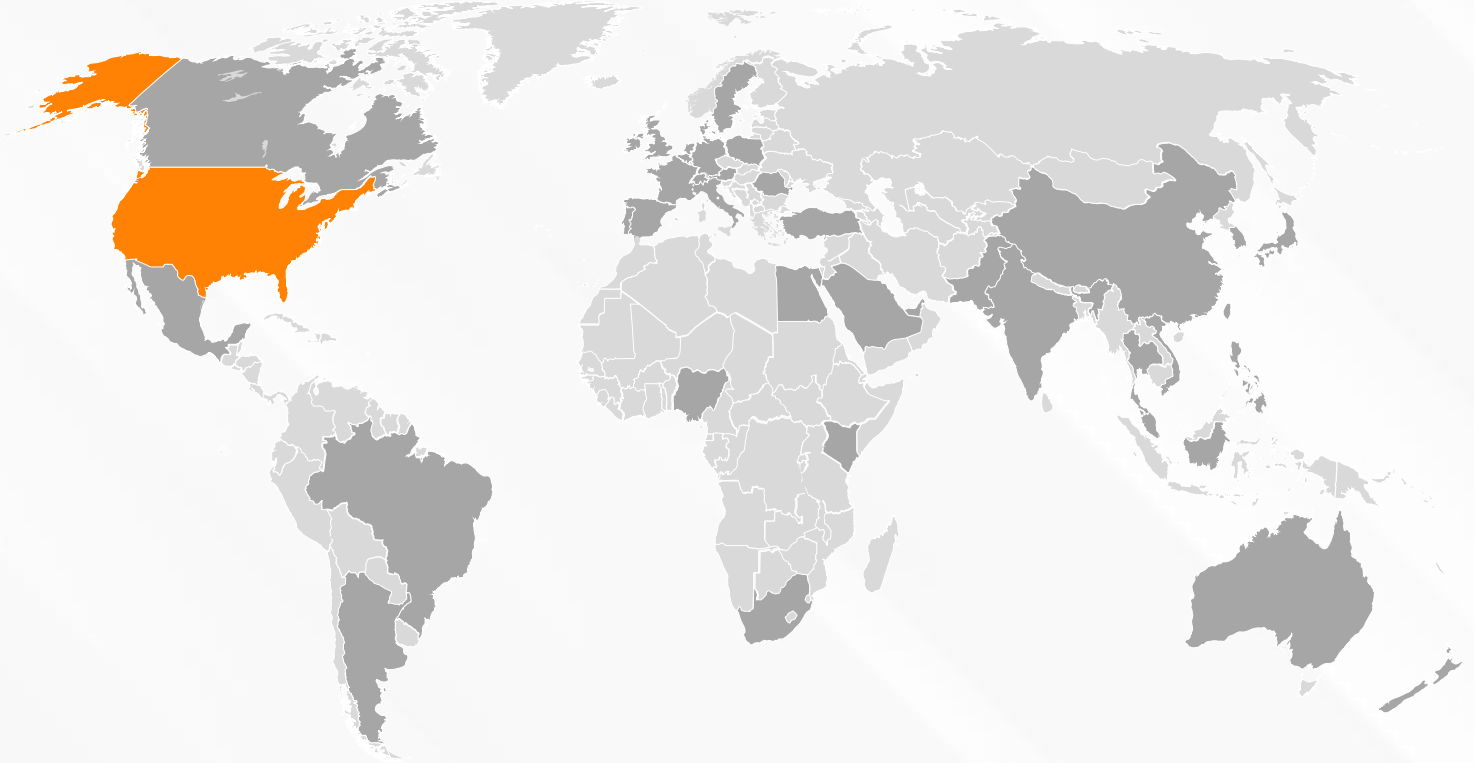
MARKETS

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Egypt
France
Germany
Hong Kong
India
Indonesia

Ireland
Italy
Japan
Kenya
Malaysia
Mexico
Netherlands
New Zealand
Nigeria
Pakistan
Philippines
Poland
Portugal
Romania

Saudi Arabia
Singapore
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Türkiye
UAE
United States
Vietnam

The data in this report will focus on findings within the
United States of America



Who we spoke to in the **United States of America**

Sample size | 2,500 people

Audience | Adults aged 18+ living in the U.S.

Weighting | Nationally representative of American adult population

Methodology | 15-minute online survey

Sample source | Online research panel

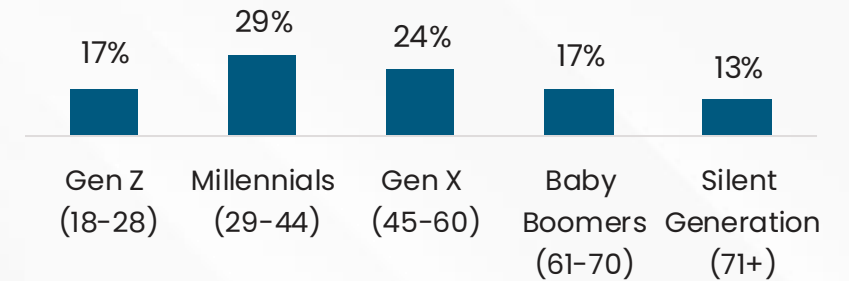
Fieldwork | 26th February – 14th March 2025

Base: All respondents U.S. (2500)

GENDER



GENERATION / AGE



WORKING STATUS

NET: Working



NET: Not working

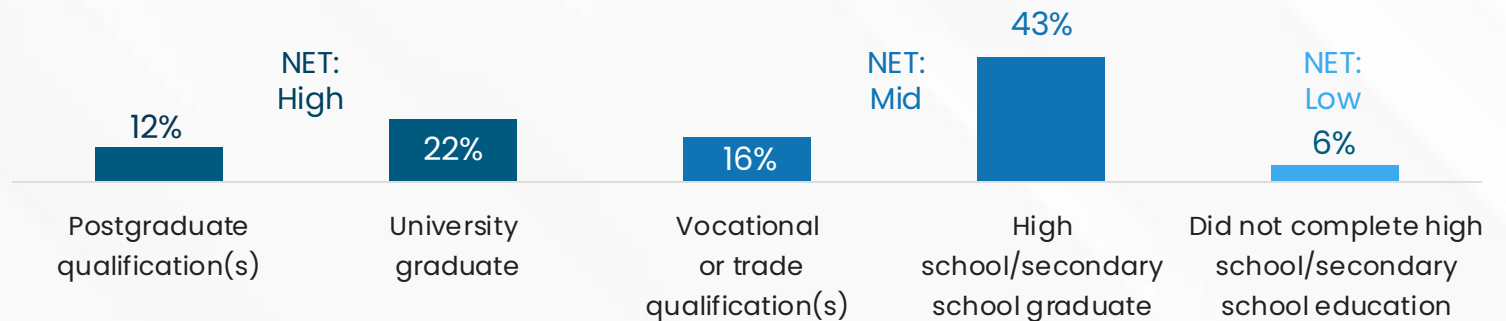
PARENTAL STATUS

NET: Parents



NET: Not parents

EDUCATIONAL STATUS



Key United States of America findings

PREVALENCE OF ENCOUNTERING A SCAM

77%

Of **American** adults have had a scam experience.

Scams are most commonly encountered on a **daily** basis, which equates to **377 scam encounters** on average per person, per year, in the U.S.

PREVALENCE OF EXPERIENCING A SCAM IN LAST 12 MONTHS

70%

Of **American** adults have had a **scam experience** in the last 12 months. Amongst this group, **Shopping scam, Fake invoice** (both 54%), and **Identity theft** (53%) are the most common type of scams experienced.

*An experience, whether successful or not for the scammer

PREVALENCE OF LOSING MONEY TO A SCAM IN LAST 12 MONTHS

22%

Of **American** adults claim to have **lost money to scams** in the last 12 months with **\$1086.7** lost to scams, per person, on average.

Funds are most commonly sent via **Debit card payment** (30%) and **PayPal** (25%).

PERCEIVED RESPONSIBILITY TO PROTECT PEOPLE FROM SCAMS

35%

Of **American** adults feel it is the responsibility of **Commercial organisations** to keep people safe from scammers, primarily the online platform used by the scammer (13%).

IMPACT OF SCAMS ON VICITM

67%

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

27% say they will be more vigilant of scams as a result.

PREVALENCE AND OUTCOME OF REPORTING TO PAYMENT PROVIDER

82%

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

44% were able to at least partly recover the money.

“

America is experiencing a scamming emergency. We are losing massive amounts of money and wasting valuable time. Our trust in financial transactions, online engagement, and the digital economy is rapidly eroding. Meanwhile, sophisticated criminal organizations based all around the world, as well as unscrupulous individuals right here at home, are reaping the rewards and stealing hard-earned income and savings from our family members, friends, neighbors, and even our kids.

We can and must do more to stem the tide. Survey respondents in this State of Scams report identify a variety of actors as responsible for stopping the scamming onslaught – financial institutions, the platforms on which they experience the scam, government agencies, police, or others. We know that no single actor can solve this problem on their own. As scamming networks grow in sophistication and effectiveness, we must do the same in response. And that’s why GASA and our country-level chapters matter today more than ever. Onward together!

Nils Mueller
GASA North America Chapter Manager

”

“

Senator Grassley opened a recent hearing with a stark warning: “Transnational organized crime groups are targeting all of us with industrial-scale fraud,” draining billions from American households to fund “drug trafficking, human trafficking, arms trafficking and other evil projects.” He emphasized: “This is a national security crisis hiding in plain sight. And we’re inadvertently funding it.”

Britain also calls fraud “a threat to national security.” Interpol issued an Orange Notice warning of imminent public safety threats. Google identifies cybercrime as a “multifaceted national security threat.”

Sophisticated criminal networks are exploiting our digital infrastructure to systematically rob Americans, and the money flows overseas to fuel more organized crime. The scale is already staggering, and the tsunami of cybercrime is likely to intensify as criminals increasingly adopt AI to impersonate with unprecedented realism.

We must treat cyber-enabled scams like the national security crisis it is by implementing four critical measures immediately.

- Appoint a White House leader to coordinate a national strategy
- Create a data fusion center for real-time threat intelligence
- Deploy countermeasures to thwart malicious ads, websites, and spoofed communications
- Create a public-private partnership that combines America’s superior technology with our government’s strong cyber defense and law enforcement capabilities


America leads the world in AI, so let’s use it to defend citizens from cyber-enabled scams. We have the technology; we just need the will.

Ken Westbrook
Founder and CEO of Stop Scams Alliance

”

The research covered **four** key topics

You can navigate through pages and sections of this report using the clickable icons in the navigation bar at the base of each slide.

Use the  button to return to this page.

 Click to navigate through sections

SCAM ENCOUNTERS

Uncovering the frequency of encountering scams, the platforms and channels used by scammers, and the prevalence, barriers and outcomes of reporting scam encounters

EXPERIENCING SCAMS

Understanding the most common scams, value lost, and the prevalence, barriers, and outcomes of reporting them

IMPACT OF SCAMS

Exploring the reasons why scams are experienced as well as the impact on wellbeing and future actions of the victim

SCAM PREVENTION

Examining consumers' self-prevention tactics and perceptions of public and commercial organisations' roles in preventing and resolving scams

To find out more about the report and its authors:

ABOUT THE REPORT

ABOUT THE AUTHORS



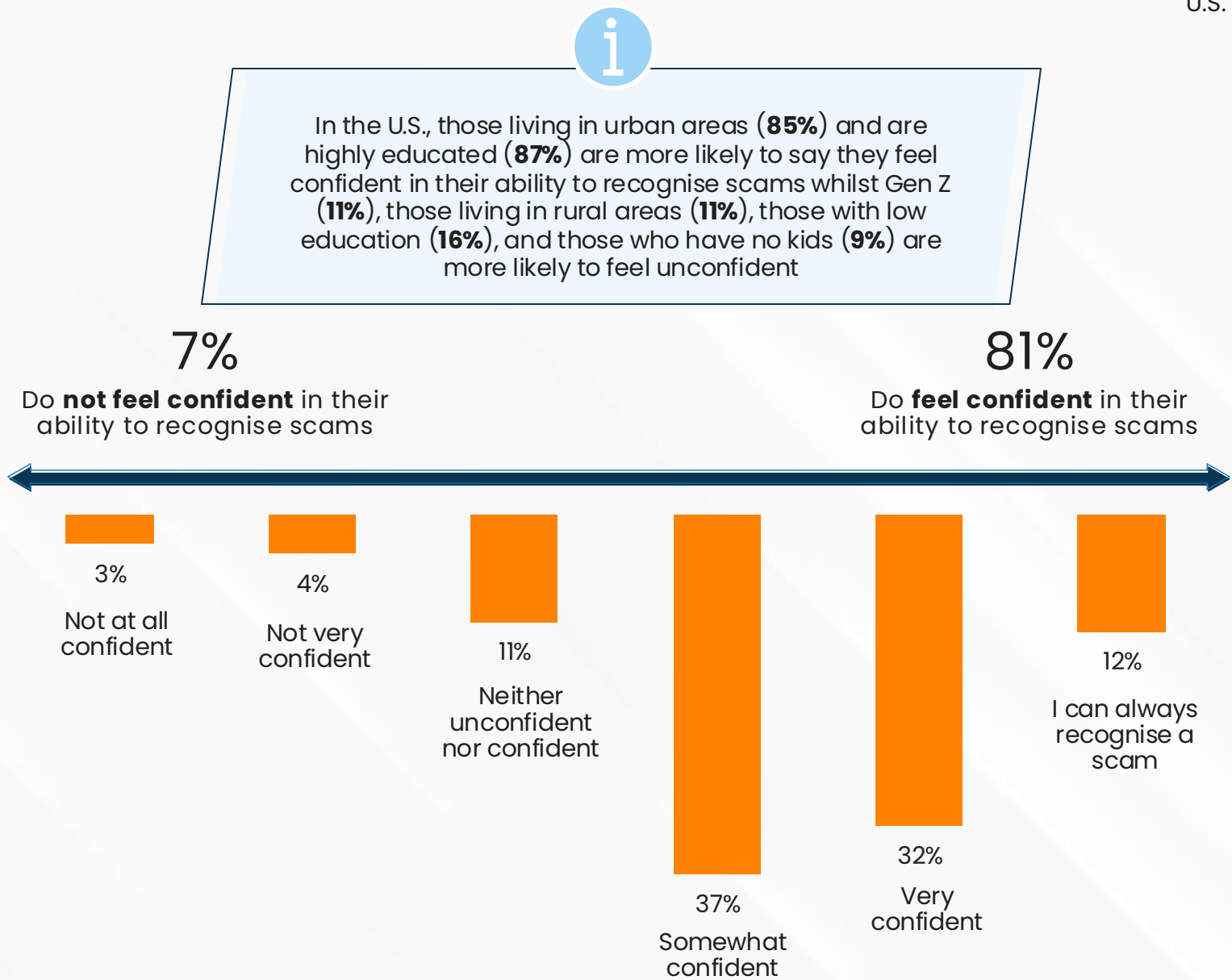
SCAM ENCOUNTERS

Uncovering the frequency of encountering scams, the platforms and channels used by scammers and the prevalence, barriers and outcomes of reporting scam encounters



Four fifths of American adults **are confident they can recognise scams**, with 12% claiming that they can “always recognise a scam”

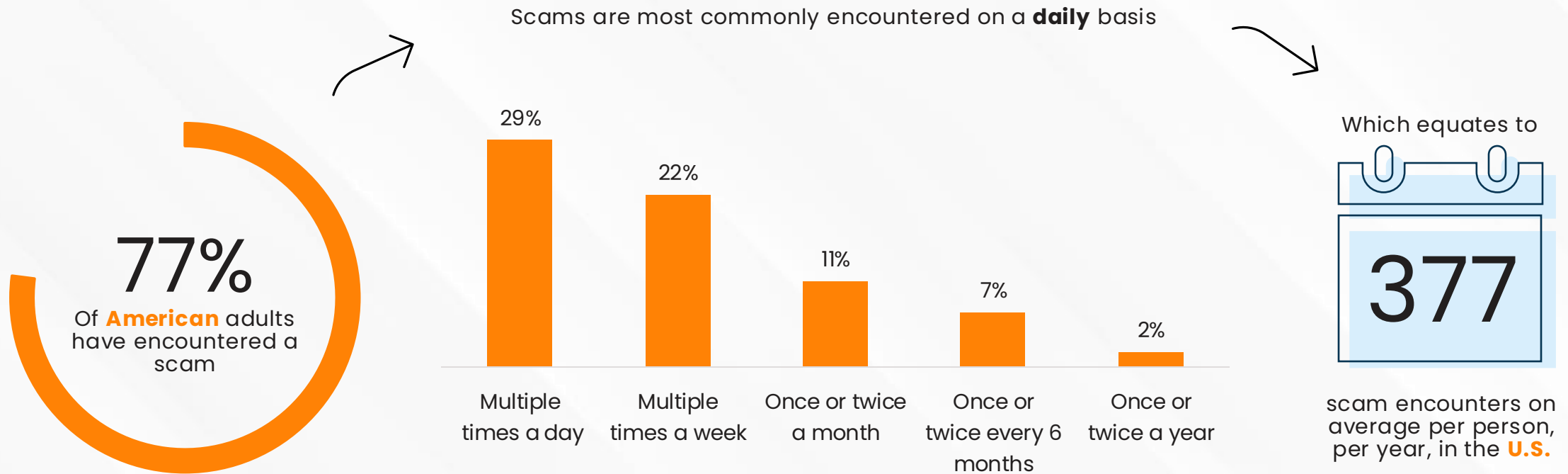
Confidence in recognising scams



Q1. How confident are you that you can recognise scams? Base: All respondents U.S. (2500)

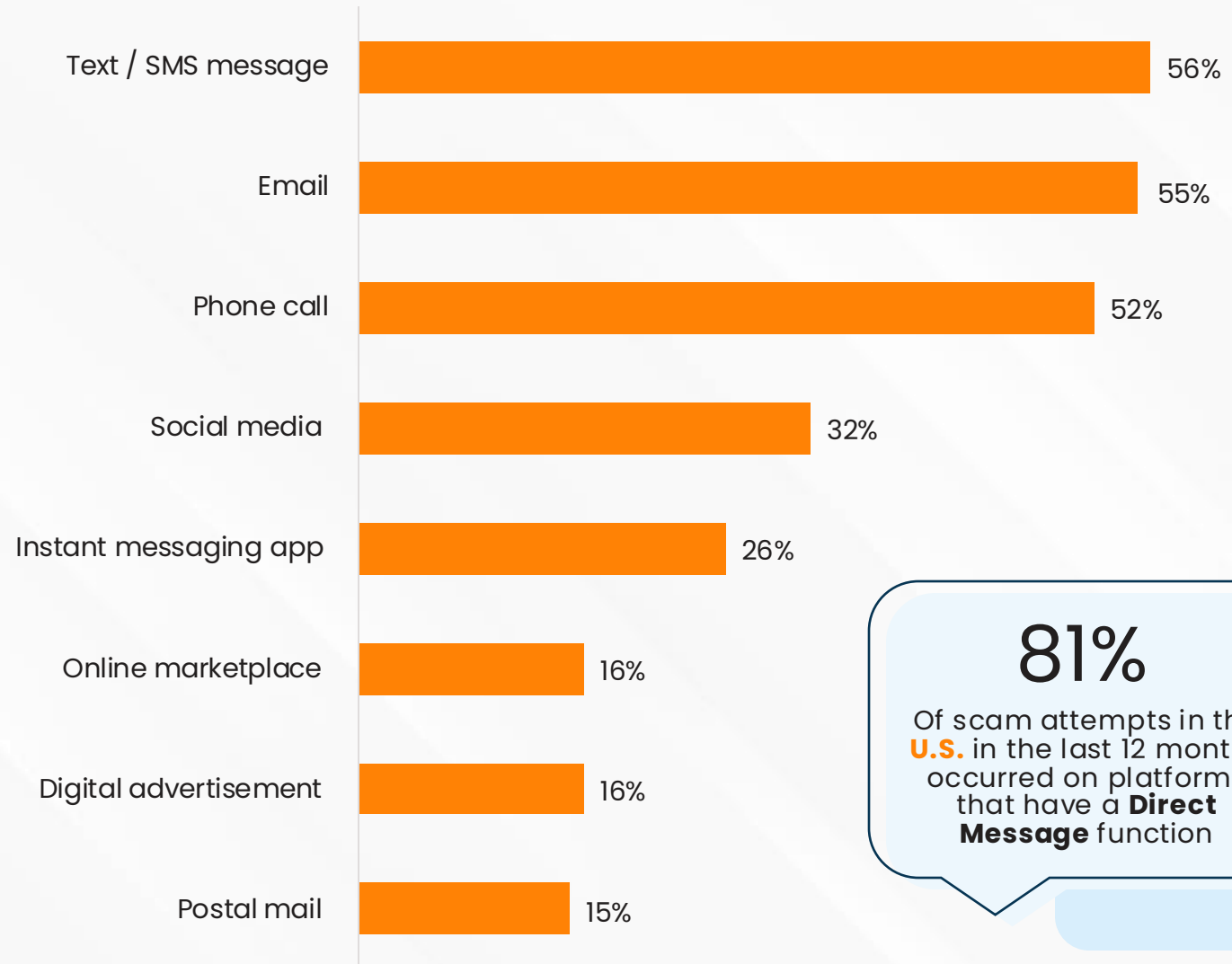
Just over three quarters of American adults say they have encountered a scam, with an average of one scam encounter happening **every day**

Prevalence & frequency of encountering a scam



Most of the scam encounters in the U.S. happen on platforms that have a **Direct Message** functionality, primarily Text message and Email

Channels used by scammers – top 8



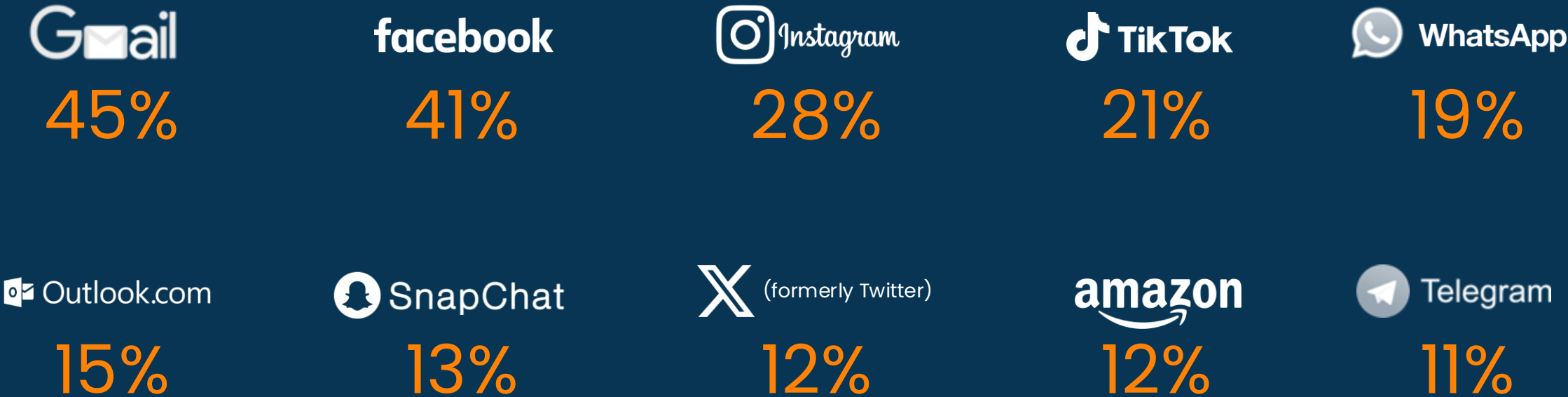
81%

Of scam attempts in the **U.S.** in the last 12 months occurred on platforms that have a **Direct Message** function

Q3. Through which communication channel(s) did scammers approach you in the last 12 months? Base: All respondents U.S. who have been exposed to a scam attempt (1764)

Gmail and Facebook are the top platforms where scam encounters occur

Top 10 online platforms used by scammers in last 12 months in the U.S.

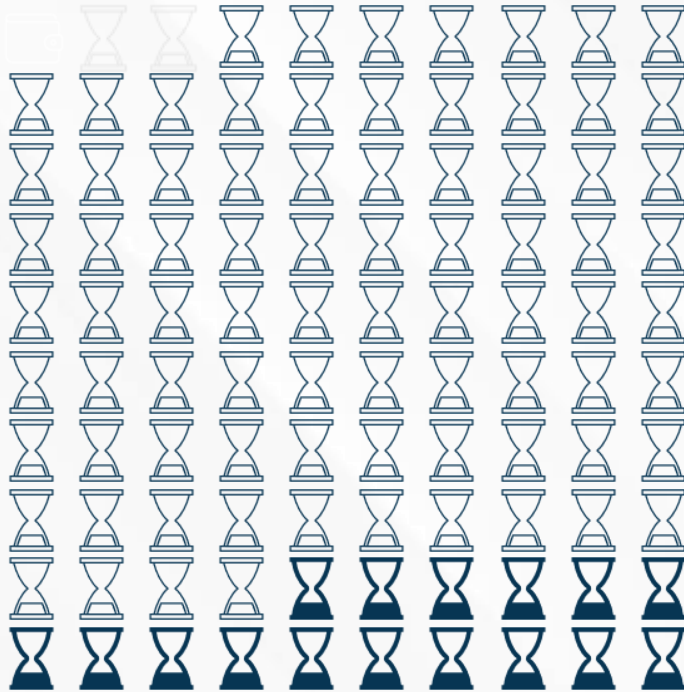


Q4A. Through which, if any, of the following global service or platform(s) did scammers contact you in the last 12 months? Base: All respondents in U.S. who have been exposed to a scam attempt (1764)

One in four American Gen Zs who experienced a scam encounter took **longer than a day** to recognise it was deceitful

Time taken to realise a scam encounter

81%
Said it took less than
a day to realise
someone was trying
to scam them



However, for **16%**
it took a day or longer
to realise...



Those in the **U.S.** who take longer to recognise a scam are more likely to be...

- Gen Z (25%)
- Millennials (21%)
- Men (19%)
- Living in urban areas (22%)
- Parents (18%)
- Top 3 platforms where they were approached by a scammer:
 - WeChat (35%)
 - Telegram (30%)
 - Roblox (29%)

Telegram, Snapchat, and X (Twitter) are platforms where it takes the longest to recognise a scam

Time taken to recognise a scam encounter, by top 10 platforms

Time taken to recognise a scam encounter, by top 10 platforms									Key =	Under index vs average	Over index vs average	
		Average across all platforms	WhatsApp	Instagram	TikTok	Telegram	Snapchat	X (Twitter)	Facebook	Gmail	Outlook Email	Amazon
Less than a day	Seconds	36%	26%	27%	26%	24%	24%	25%	36%	45%	46%	27%
	Minutes	36%	34%	37%	36%	29%	31%	32%	39%	37%	37%	34%
	Hours	10%	14%	15%	15%	17%	17%	15%	8%	8%	6%	16%
A day or longer	Days	9%	13%	11%	10%	16%	12%	13%	8%	5%	4%	10%
	Weeks	4%	7%	5%	5%	5%	7%	6%	4%	2%	3%	6%
	Months	2%	1%	3%	3%	5%	4%	4%	2%	1%	1%	3%
	About a year	1%	2%	1%	2%	2%	2%	2%	1%	0%	1%	2%
	More than a year	1%	1%	1%	1%	2%	1%	1%	0%	0%	1%	1%

74%

Of those who have been exposed to scams in the **U.S.**, **have reported a scam encounter in the last 12 months**

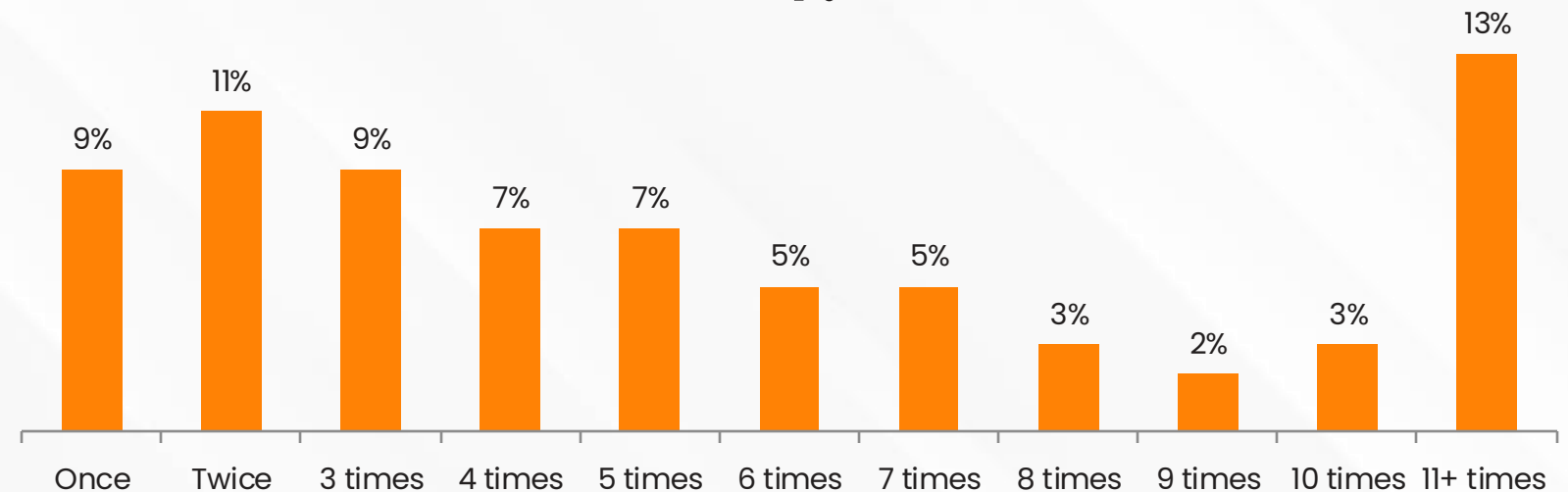


Higher amongst Gen Z (79%), Millennials (78%), men (76%), those living in urban areas (78%), those with a higher level of education (77%) and those who are parents (76%)

Three quarters of Americans who encountered a scam have reported it **at least once**

Frequency of reporting a scam encounter in the last 12 months

Each person has **reported 4.2** scam encounters on average, in the last year, **in the U.S.**



Q5. How many times, if any, have you reported a scam attempt to the service or platform provider where you experienced the scam attempt in the last 12 months?
Base: All respondents in U.S. who have been exposed to a scam attempt (1706)

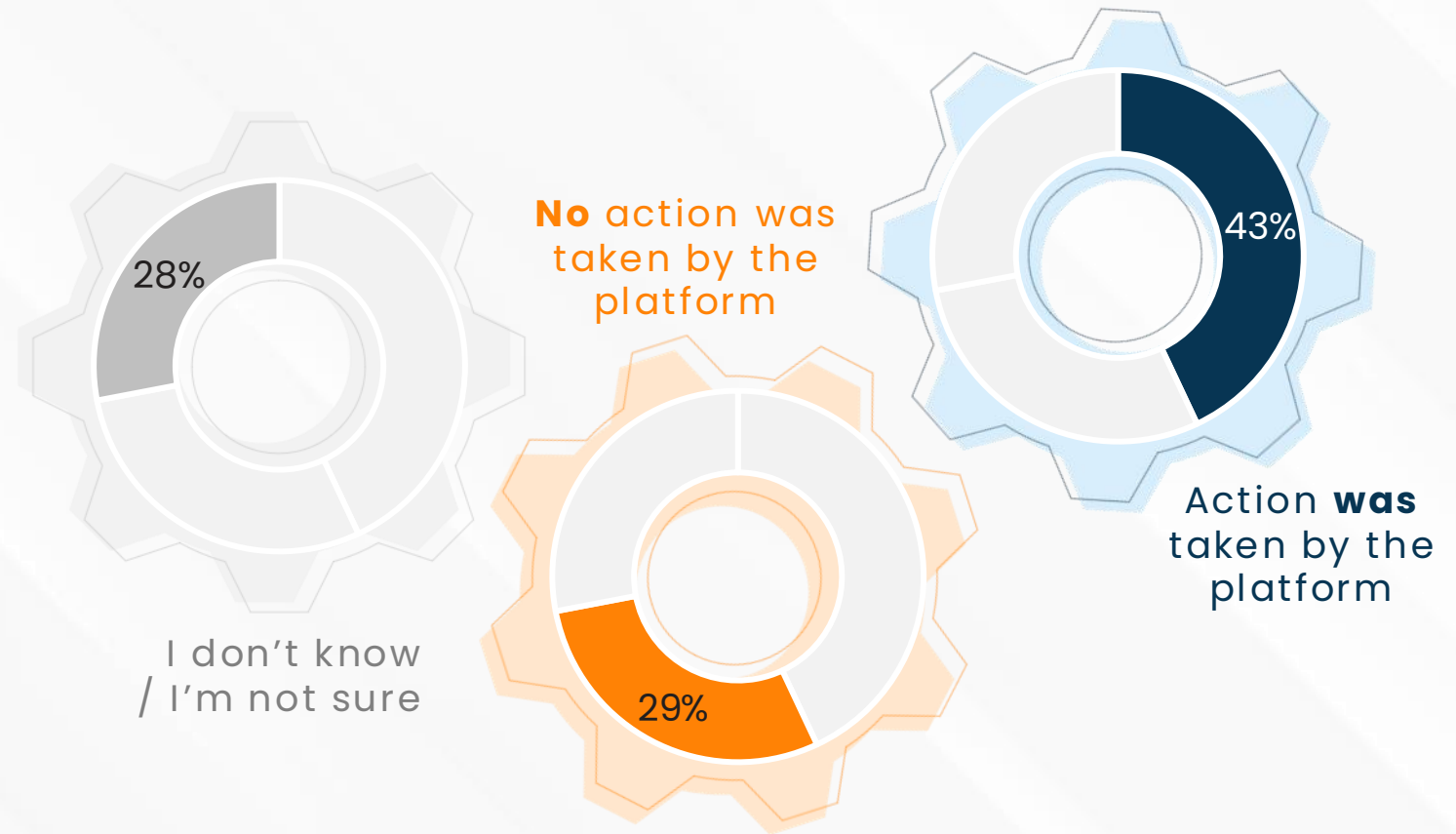


57%

Of those reporting a scam in the last 12 months in the **U.S.** say that either **no action was taken (29%)** or they aren't sure what the outcome (28%)

Almost three fifths say **no action was taken by the platform** when they reported the scam encounter

Outcome of reporting scam encounter to platform / service provider



Q6. What happened when you reported the scam attempt to the platform or service provider? Base: All respondents in U.S. who have reported a scam attempt in the last 12 months (1253)

...which is one of the main reasons scam encounters don't get reported, along with being unsure whom to report the scam to

Barriers to reporting scam encounters



The barriers for the **21%** who have never reported a scam attempt in **the U.S.** are...





EXPERIENCING SCAMS

Understanding the most common scams, value lost, and the prevalence, barriers, and outcomes of reporting them



Seven in ten American adults have had a scam experience in the last 12 months

Prevalence of experiencing a scam in last 12 months



of **American** adults claim to have been scammed in the last 12 months

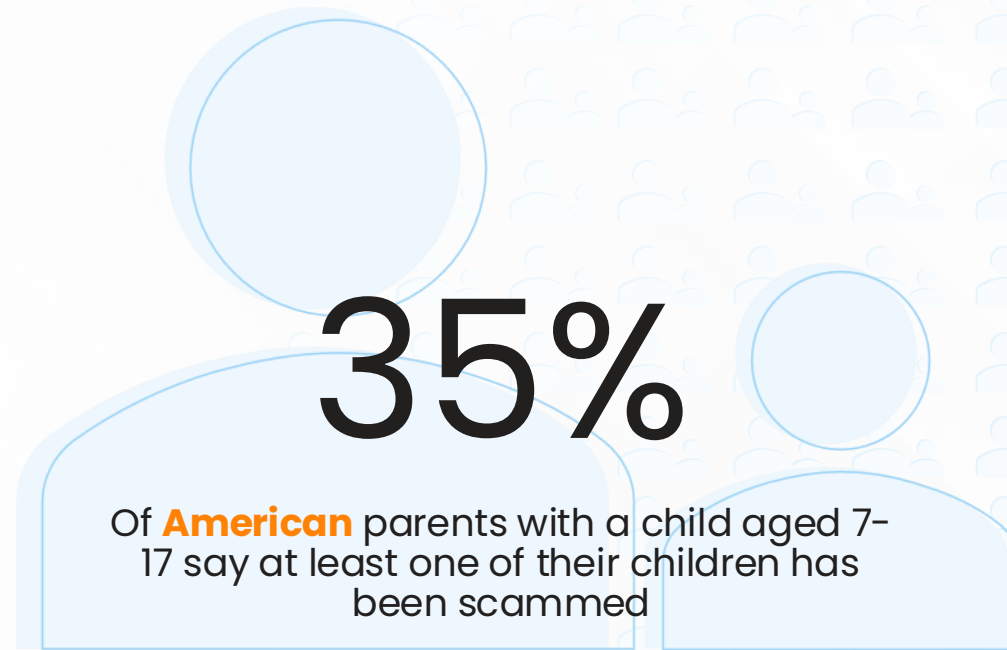
Those most likely to have experienced a scam are...

Those living in suburban areas	73%	Parents	74%
Those who are confident in their ability to recognise a scam	75%	High level of education	80%



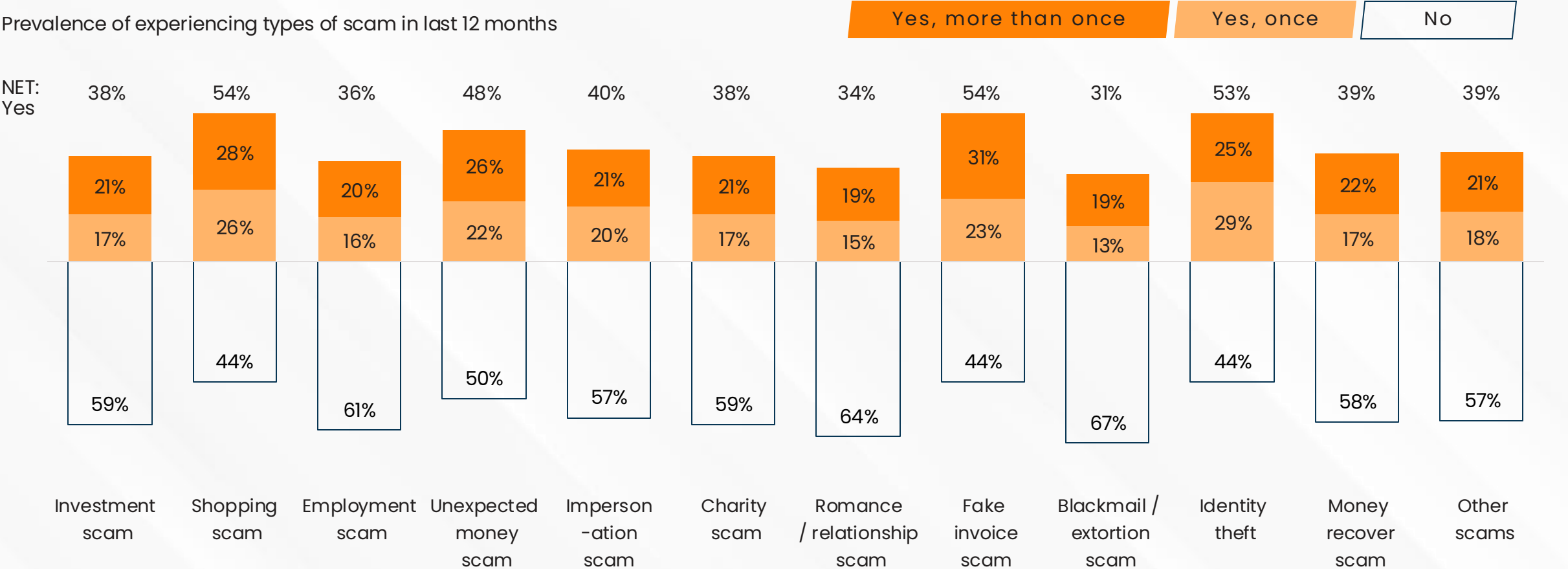
And just over a third of parents say **their children** have experienced at least one scam too

Proportion of parents reporting scam experiences amongst their children



Q23. Have any of your children between the age of 7-17 been scammed? Base: All U.S. respondents who have children aged 7-17 (440)

Shopping, fake invoice, and identity theft scams are the most experienced types of scam in the U.S., affecting more than half of those who have been targeted



[Click here to review full scam descriptions seen by respondents within the survey](#)

Q8. Have any of the following scams happened to you in the last 12 months? Base: All U.S. respondents who have been contacted by scammers (1764)



Someone in New Mexico had stolen my identity was using my name and information to sign up for services, then never making payments.
Identity theft

By phone call about owing a bill or something I purchased and it was waiting for delivery information. Also toll fees I owed but I don't live in a city with tolls.
Fake invoice scam

With some having money stolen on **Facebook** and via **fake invoices**

Scam victim description of experience

It was on Facebook marketplace, selling grinch personalized stockings paid \$100 for 6 of them but never received them and was blocked by the seller.
Shopping scam

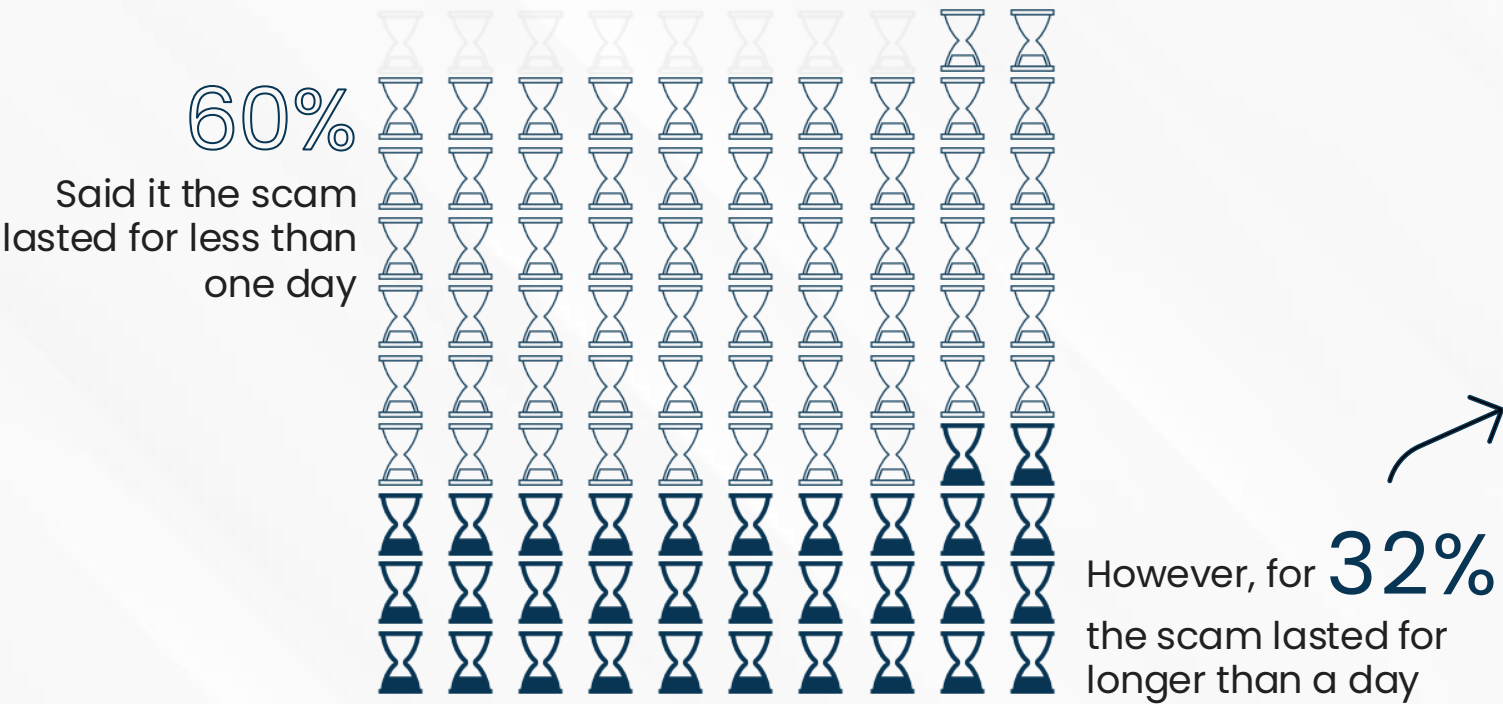
They claimed I was a winner of the lottery and I had to pay them a fee of \$250 for the money to be sent to me
Unexpected money scam



Q9. Please describe the scam you experienced in the last twelve months. Base: All U.S. respondents who have been scammed (1743)

Nearly a third of American scam victims said it lasted longer than a day

Length of scam



i Those in the **U.S.** whose scams lasted longer than a day are more likely to be...

Gen Z (42%)

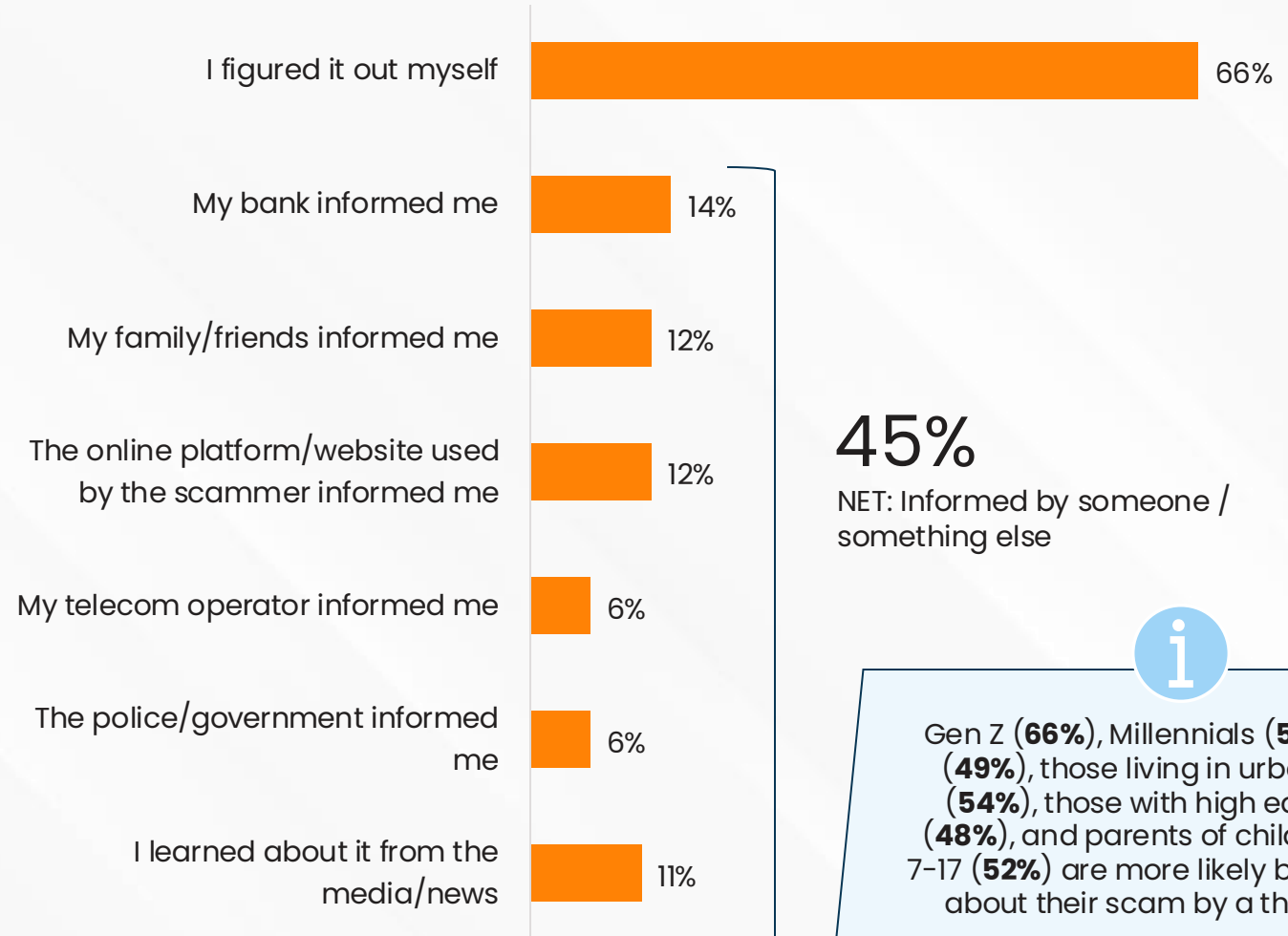
Those living in an urban area (38%)

Parents of children aged 7-17 (39%)

[Click here to see length breakdown by scam type](#)

Most realised they had been scammed by figuring it out for themselves

How victim discovered they were scammed



Q12. How did you discover you were scammed? Base: All U.S. respondents who have scammed (1743)

**\$64.8 billion
has been stolen by
scammers in the
U.S. in the last year**

Value lost to scams

22% of **American** adults claim to have lost
money to scams in the last 12 months



\$1086.7

Stolen from the average victim
in the **U.S.** in the last 12 months

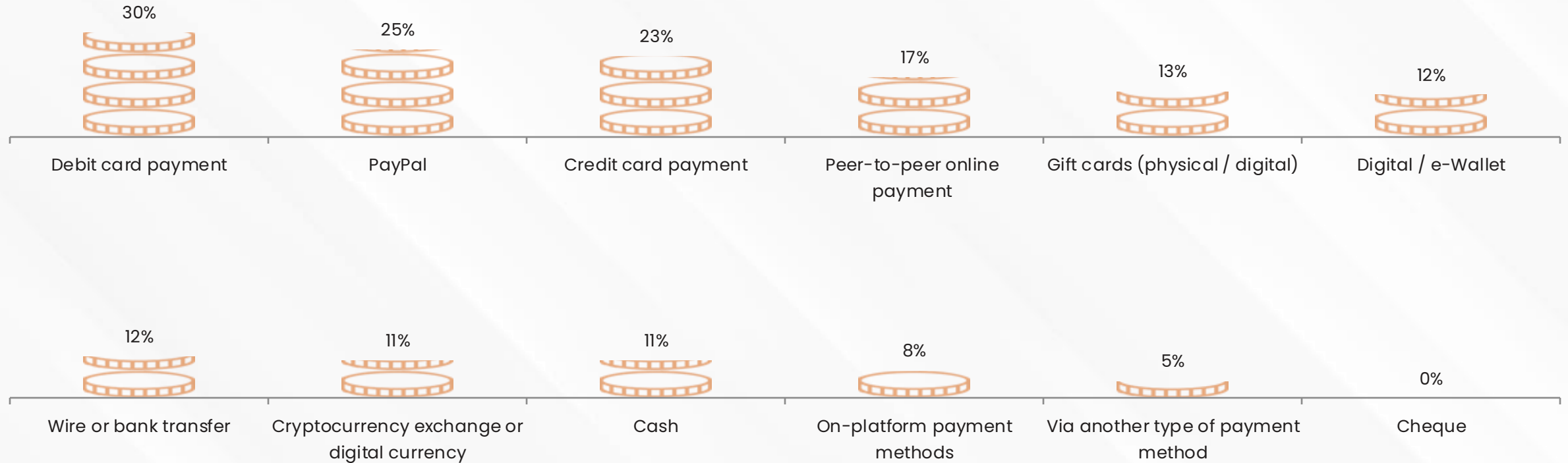


Gen X tend to have more stolen on average (**\$1405.3**) vs Baby Boomers (**\$681.7**). Those who 'can always recognise a scam' have had **\$1406.4** stolen on average in the last year in the U.S.



With **debit card payments** and **PayPal** being the most common methods of transferring the money

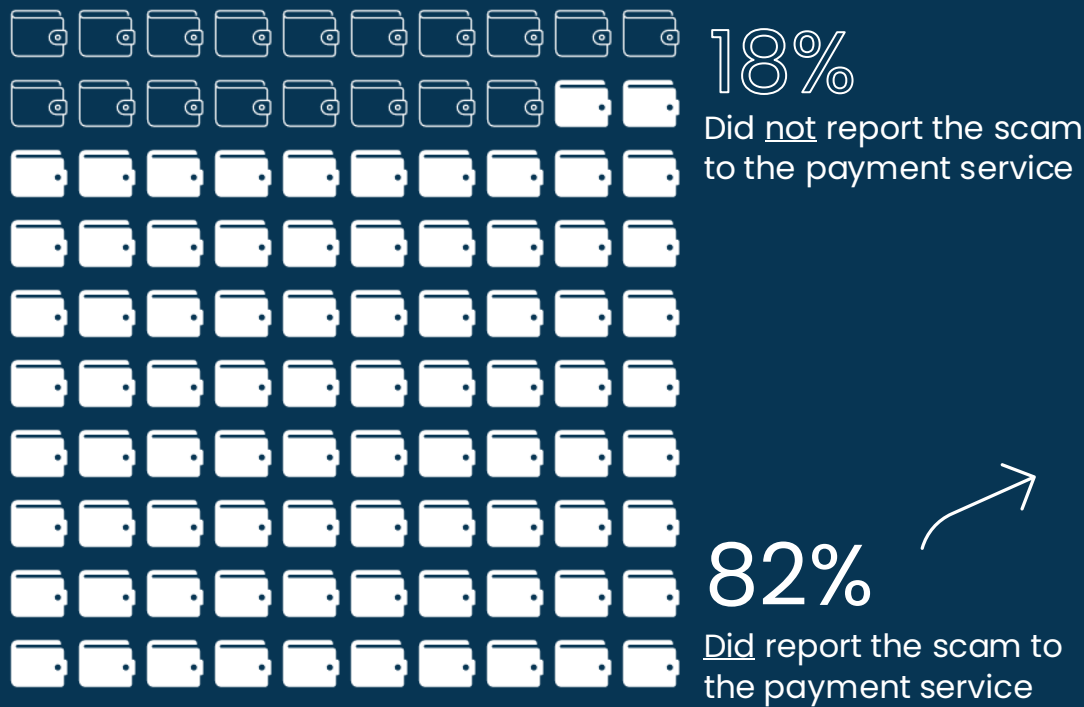
Payment channels scammers received the payment



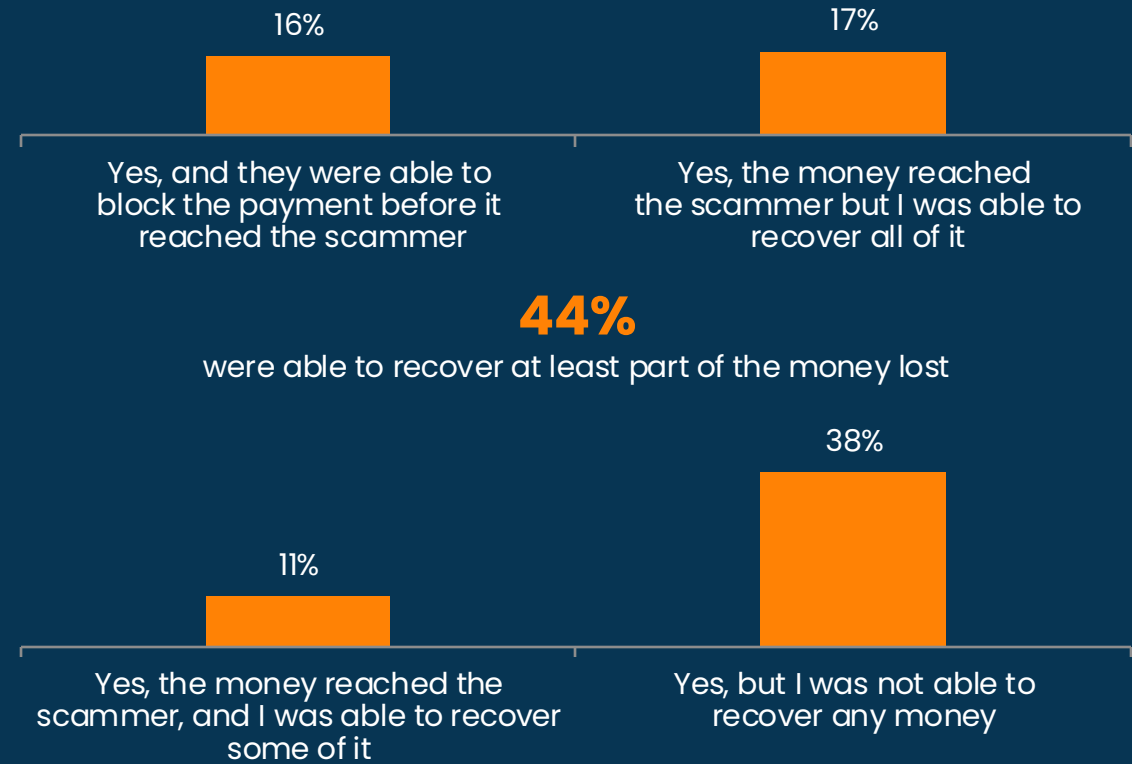
Q14. How did the scammer receive your money? Base: All U.S. respondents who have been scammed and lost money (547)

Just over four in five reported their scam to the payment service, and over two fifths said their money was at least partially recovered

Did you report the scam to the payment service?

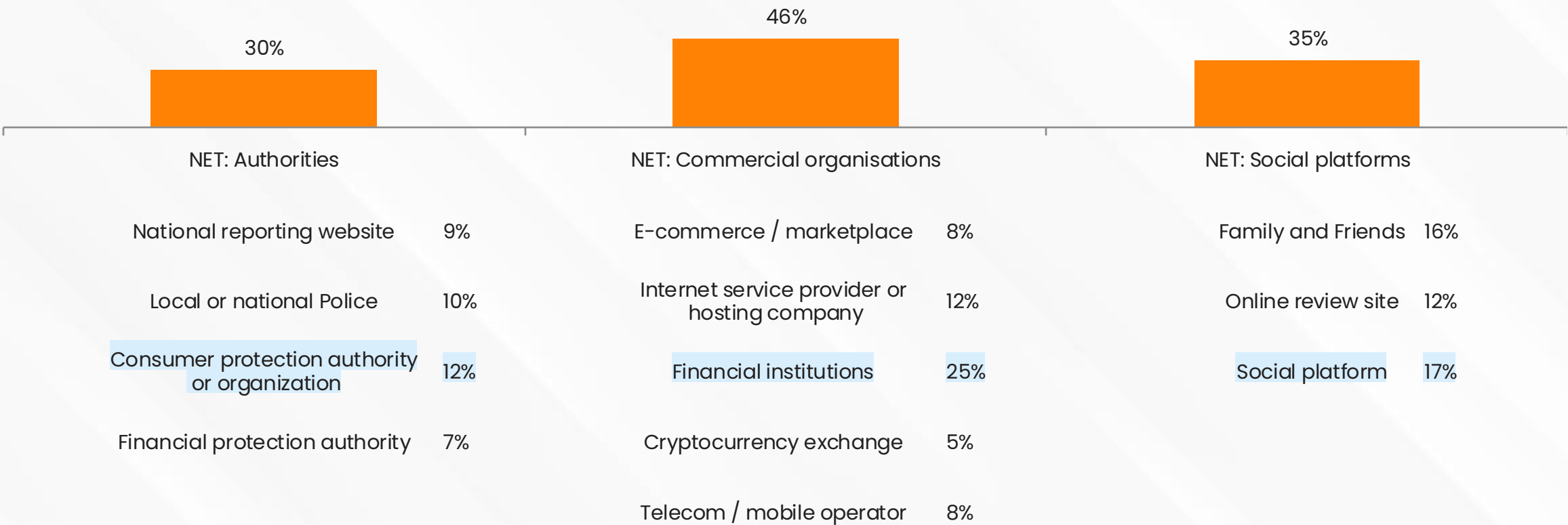


Recovery outcome



Scams were more likely to be reported to commercial organisations than they were authorities

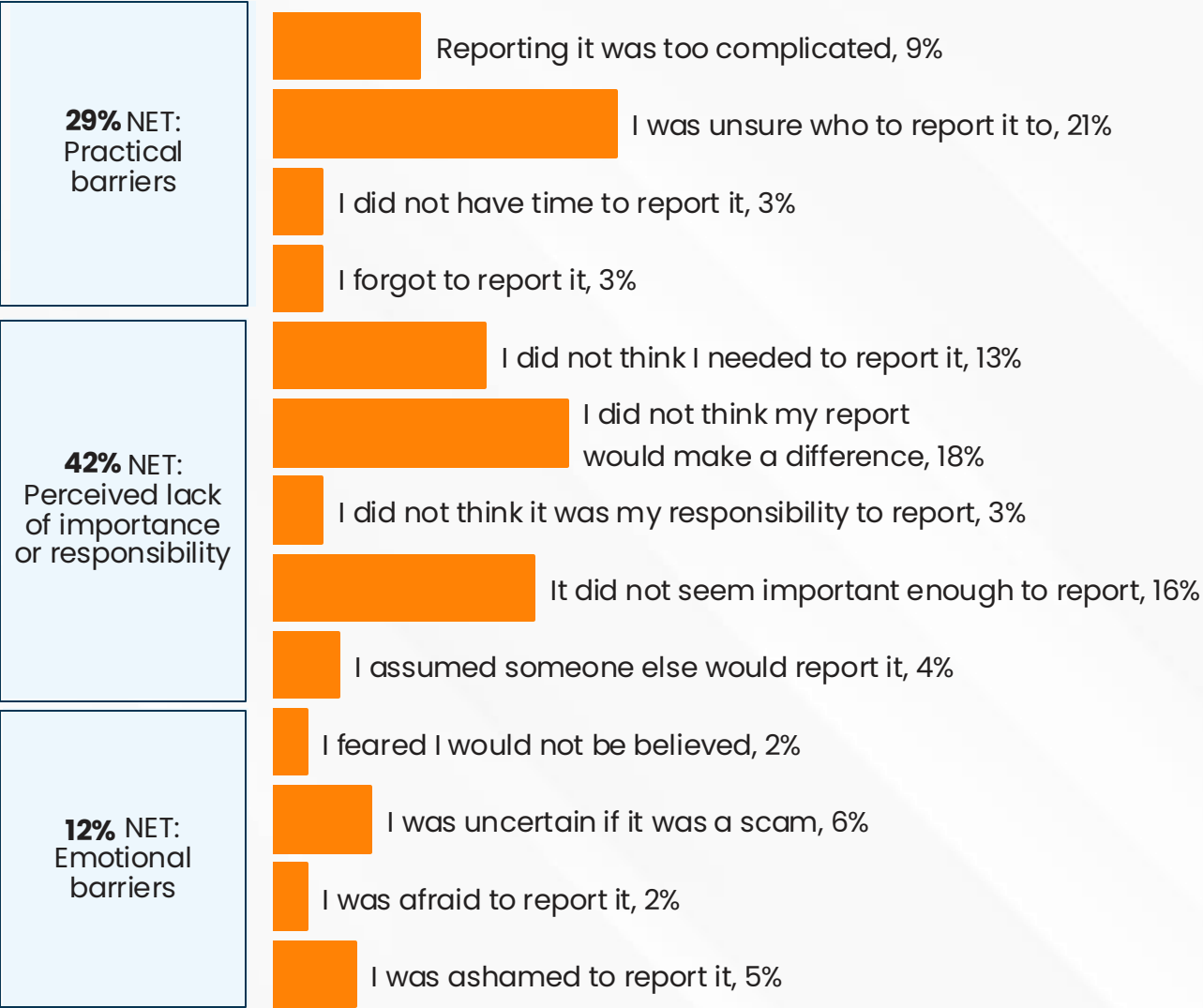
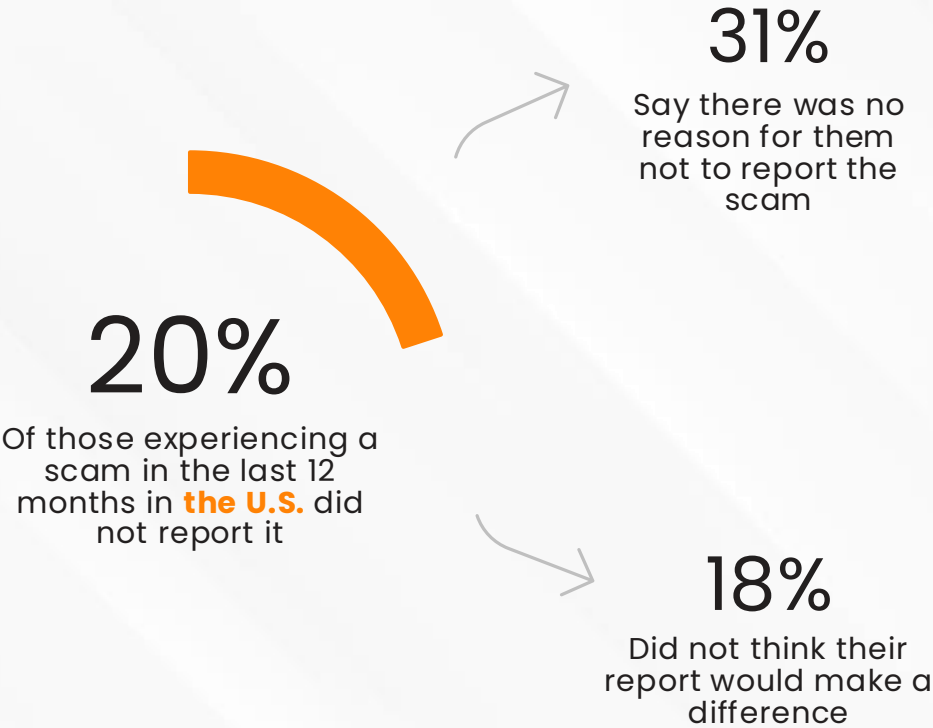
Channels / organisations scams reported to – top 10



Q21. Who did you report the scam to? Base: All U.S. respondents who have been scammed (1743)

Reasons not to report scams were the **same reasons** for not reporting scam encounters

Barriers to reporting scams



Q21. Who did you report the scam to? Base: All U.S. respondents who have been scammed (1743) Q22. Why didn't you report the scam? Base: All U.S. respondents who did not report the scam they experienced (358)



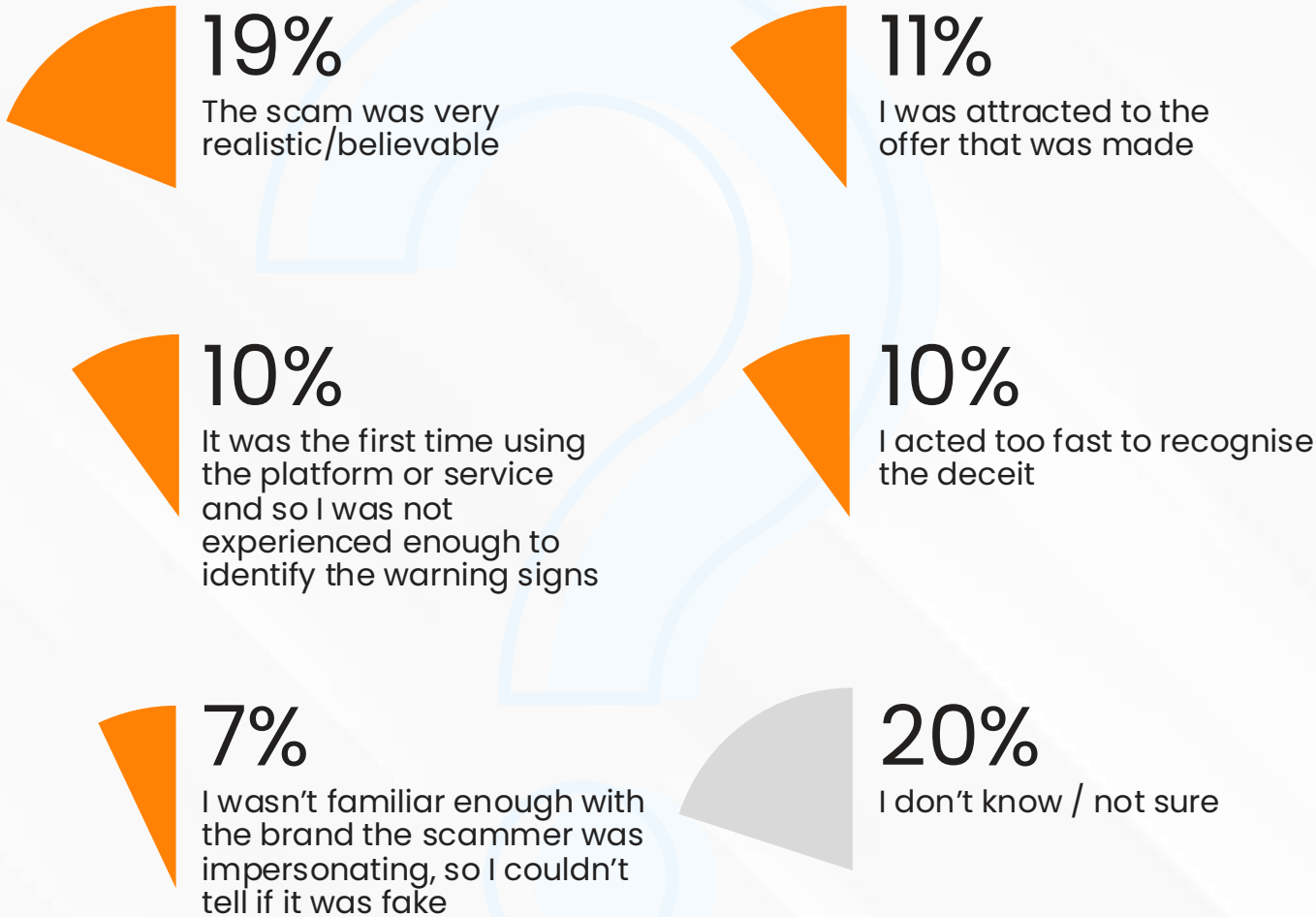
IMPACT OF SCAMS

Exploring the reasons why scams are experienced as well as the impact on wellbeing and future actions of the victim



The believability of the scam is the main reason why American victims think they were scammed

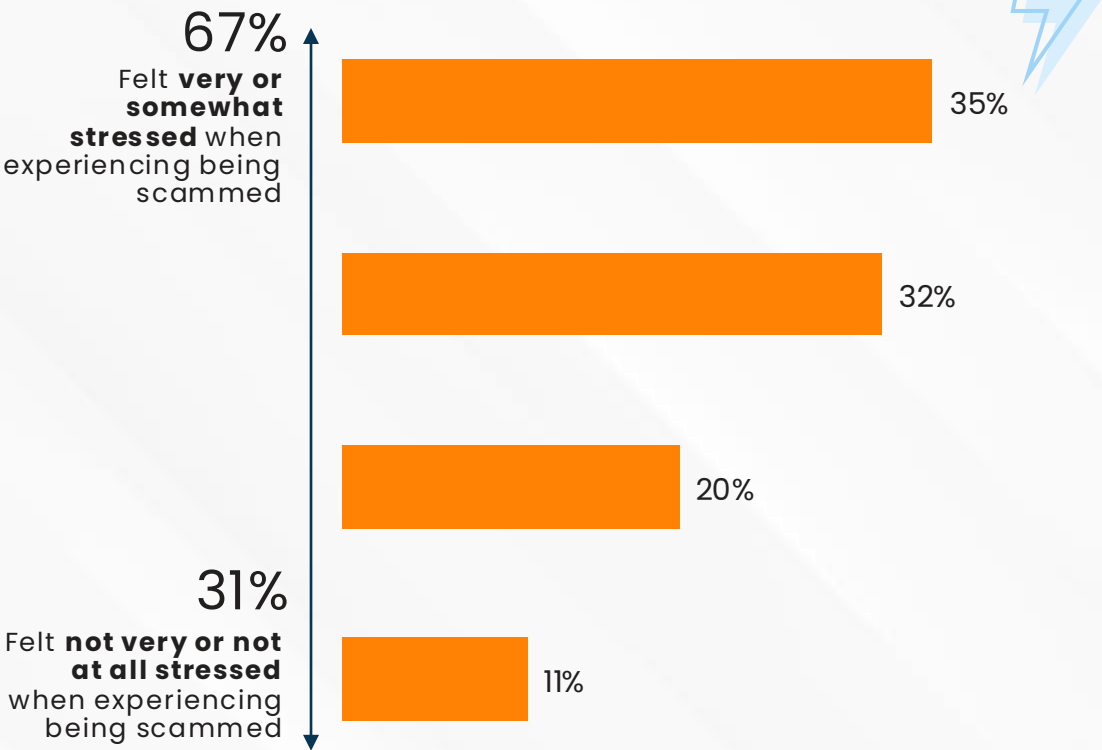
Reasons why scams experienced – top 5



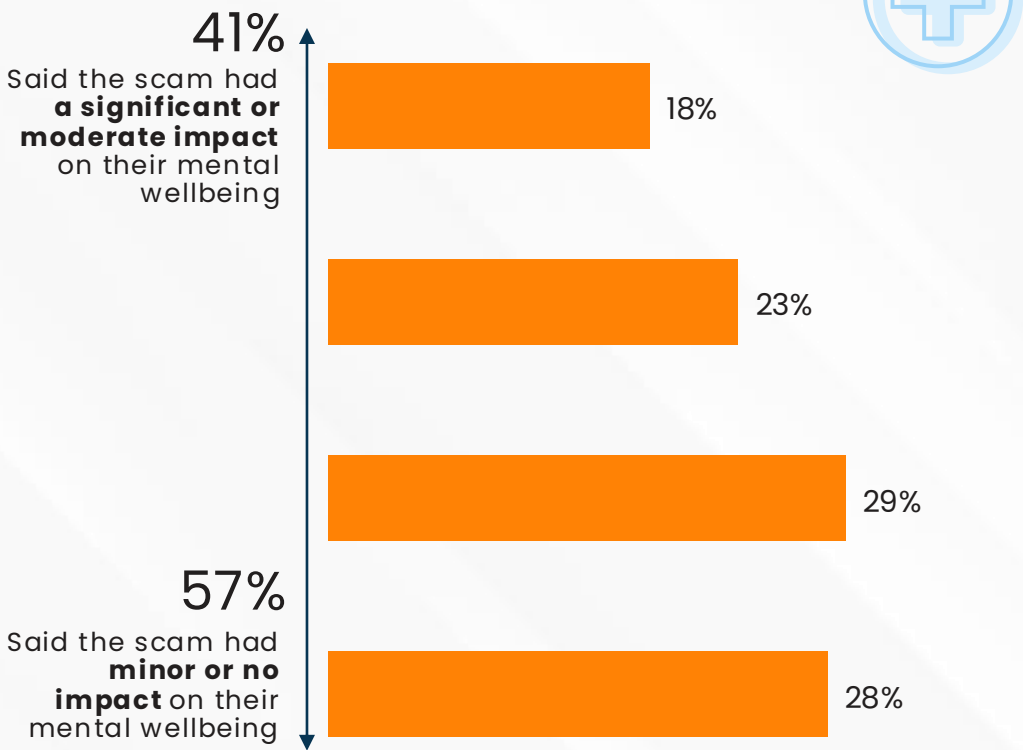
Q19. Why do you think you were scammed? All U.S. respondents who have been scammed (1743)

Two fifths of those scammed said it impacted their wellbeing, and the majority said it made them feel stressed

Impact of being scammed on stress



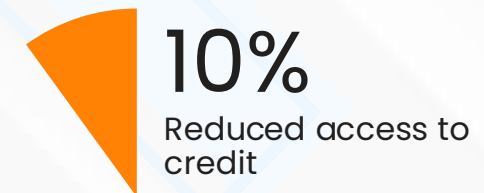
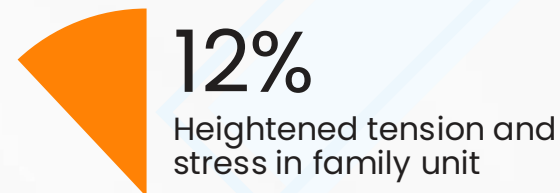
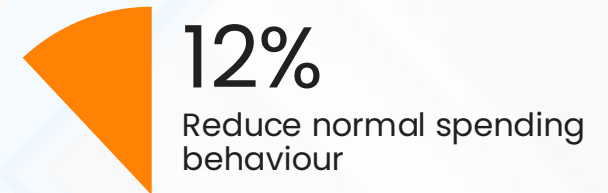
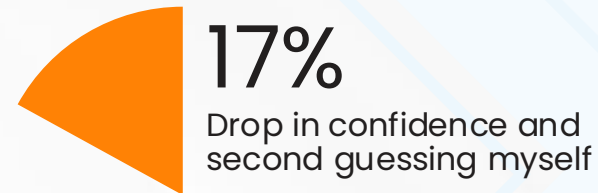
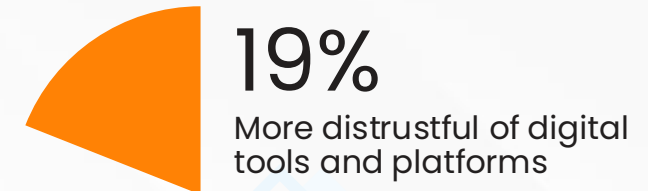
Impact of being scammed on mental wellbeing



Q16. To what extent was experiencing the scam stressful? Q17. To what extent did the scam impact your mental wellbeing? Base: All U.S. respondents who have been scammed (1743)

Whilst being scammed increases vigilance to future encounters, one in eight say they **had to reduce normal spending behaviour as a result**

Impact of scams on those experiencing family – top 6



Q18. How has the scam(s) impacted you and your family? Base: All U.S. respondents who have been scammed (1743)



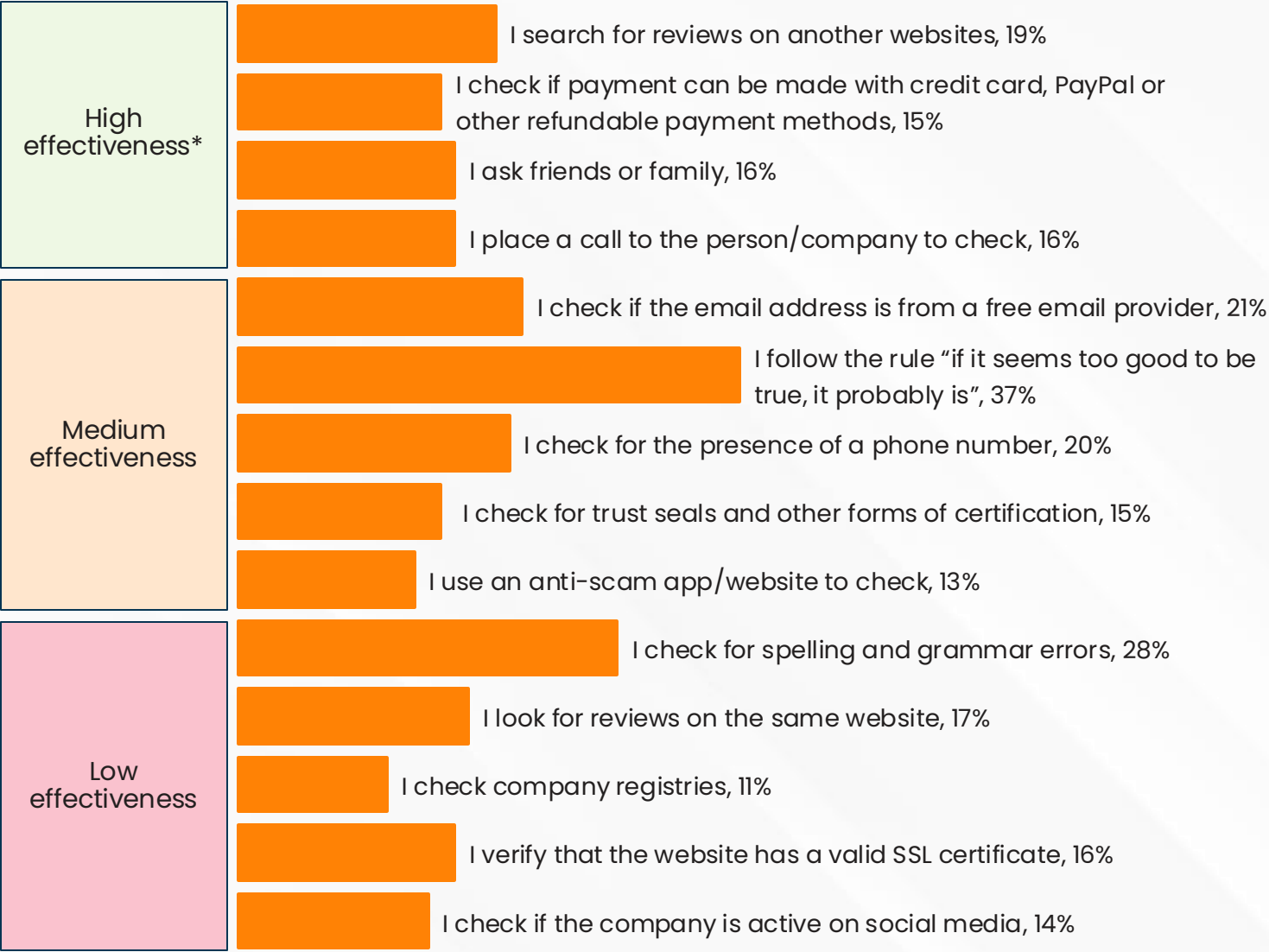
SCAM PREVENTION

Examining consumers' self-prevention tactics and perceptions of public and commercial organisations' roles in preventing and resolving scams



Over a quarter of American adults check spelling and grammar errors to legitimise an offer, but this has low effectiveness

Steps taken to check legitimacy of offer



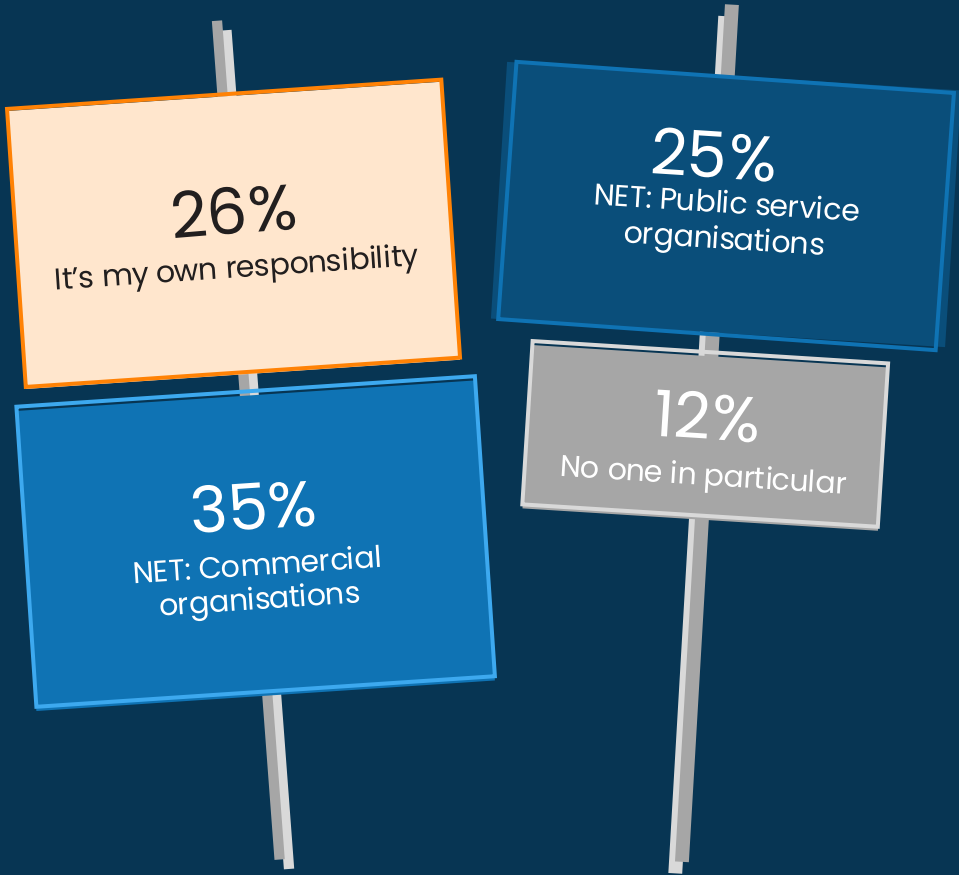
Q20. What steps do you take to check if an offer is real or a scam? Base: All U.S. respondents (2500) *Effectiveness groupings provided by GASA

American adults place the responsibility of keeping people safe from scams on **commercial organisations**, primarily the online platform

Responsibility for keeping people safe from scammers ranking:

13%	The online platform used by the scammer (e.g., social media, email, messenger)
10%	The website provider / hosting company used by the scammer
9%	The government
8%	Consumer protection authorities
7%	My bank, payment method or crypto exchange
5%	The police
4%	Financial protection authorities
4%	My telecom or mobile operator
2%	Insurance companies

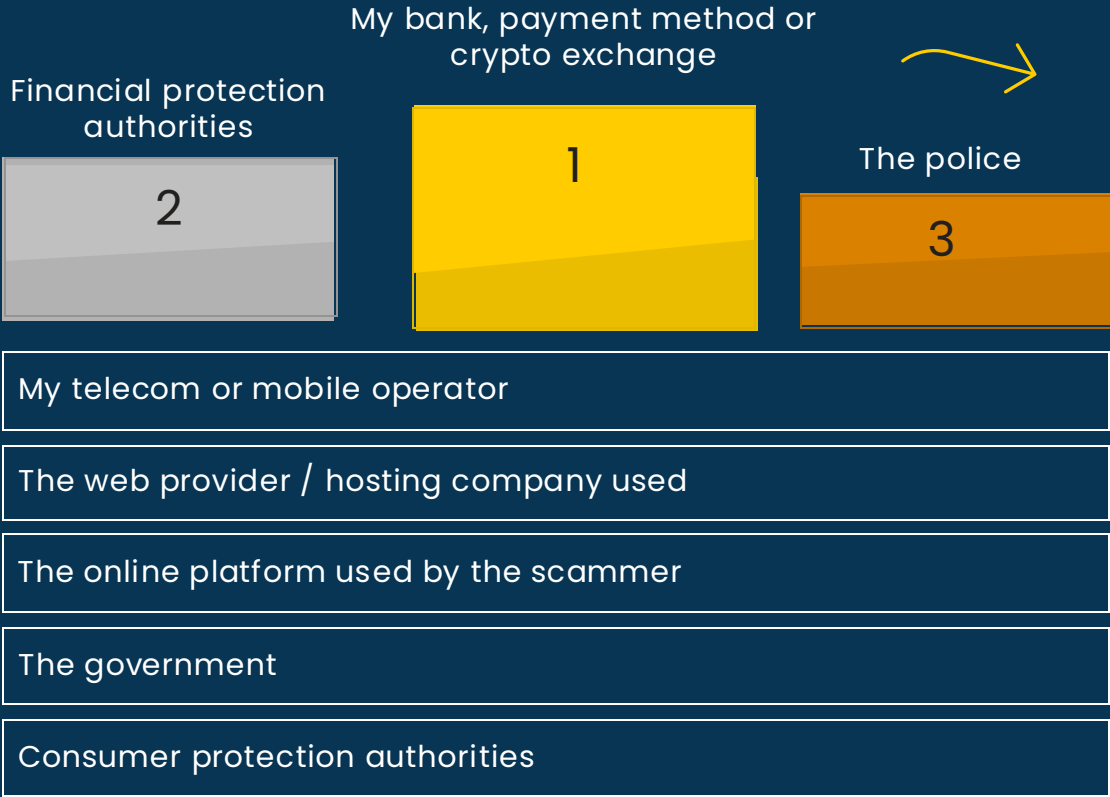
Most responsible
Least responsible



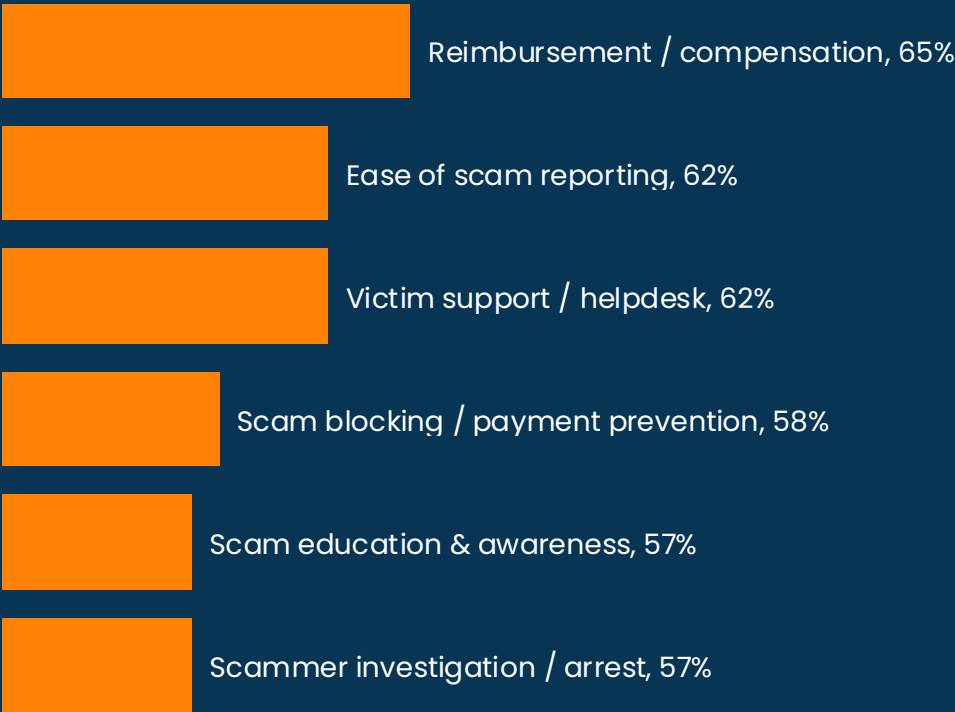
Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All U.S. respondents (2500)

Meanwhile, banks, payment methods, or crypto exchanges are rated highest amongst American adults for preventing or resolving scams

Performance ranking on preventing / resolving scams



My bank, payment method or crypto exchange –NET: Good:



[Click here to see full ratings](#)

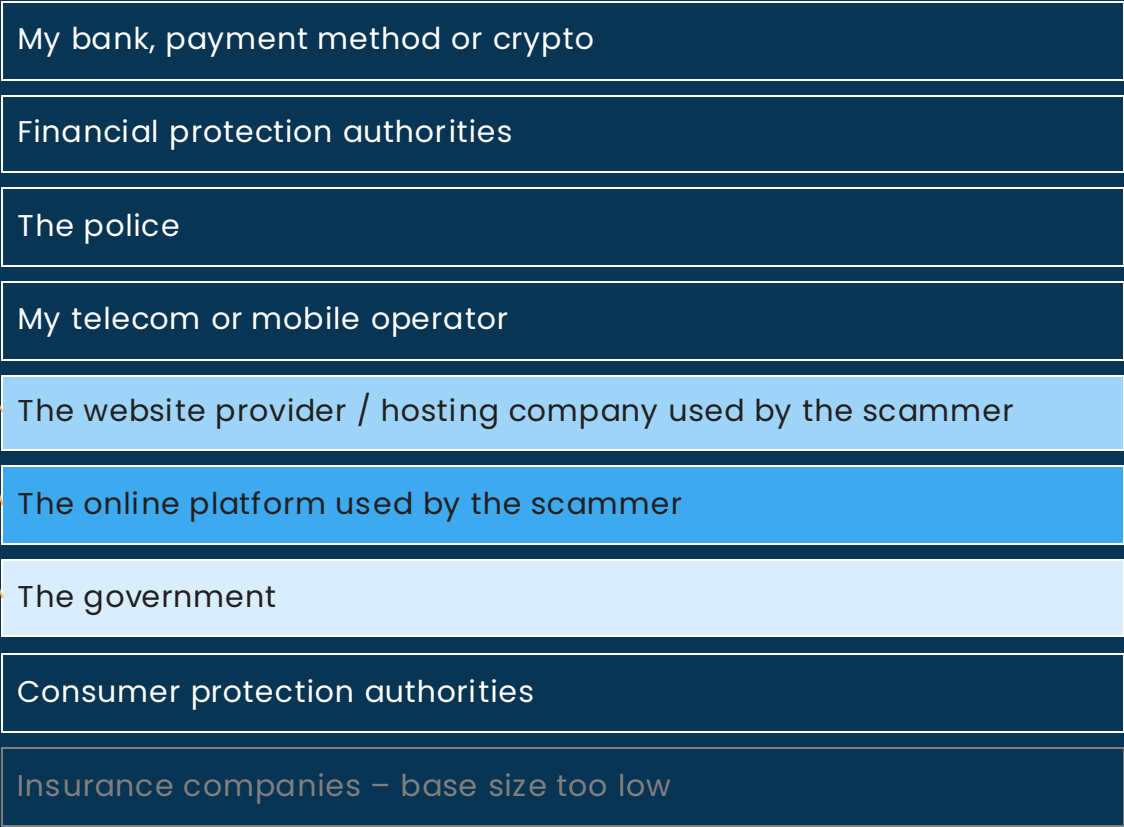
Q25. You said [banks, payment methods or crypto exchanges] should be most responsible for keeping people safe from scammers. How do you rate [banks, payment methods or crypto exchanges] on the following aspects: Base: All U.S. respondents who think someone else should be responsible for keeping people safe from scammers (1503), those who think Banks, payment methods or crypto exchanges should be most responsible (169)

American adults expect **online platforms** to protect users from scams but see them as less effective than other organisations

Responsibility for keeping people safe from scammers ranking:



Performance ranking on preventing / resolving scams:



Q24. Who do you think should be most responsible for keeping people safe from scammers? Base: All U.S. respondents (2500) Q25. You said should be most responsible for keeping people safe from scammers. How do you rate on the following aspects: Base: All U.S. respondents who think someone else should be responsible for keeping people safe from scammers (1503)

Almost half of American adults believe **banks** and **credit card companies** should always be responsible for reimbursing those experiencing a scam

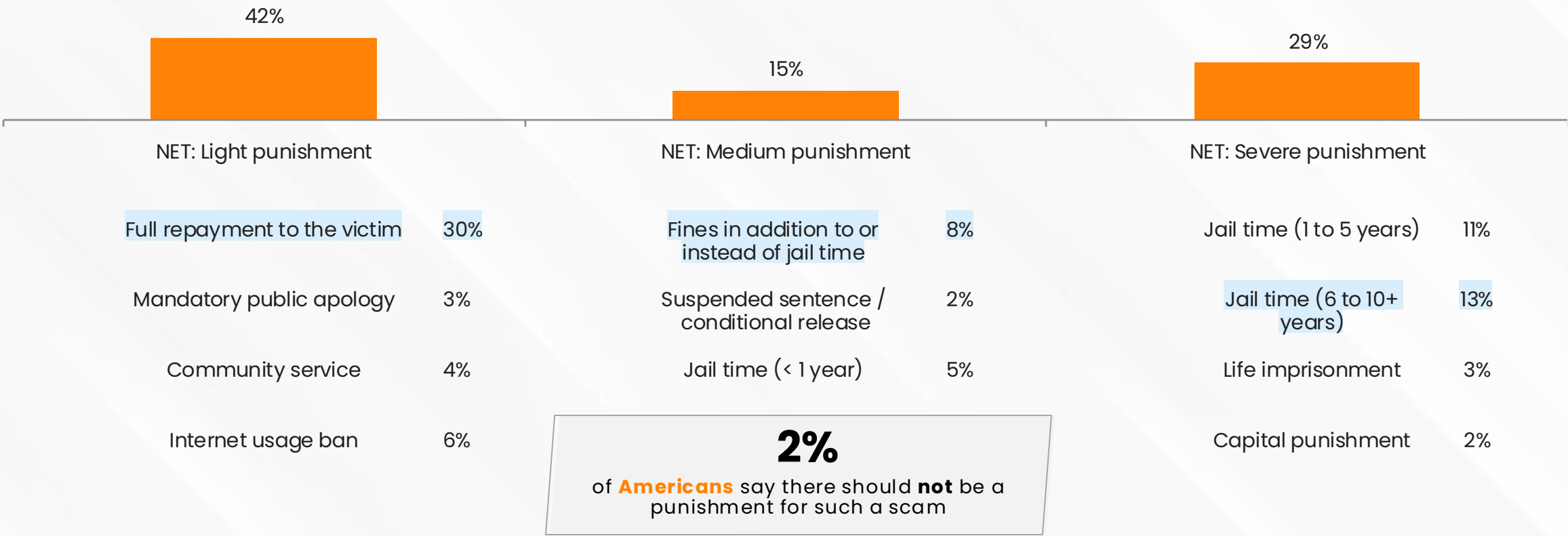
Level of expected responsibility for reimbursing scams – top 3 platforms



Q26. If someone is scammed on any of the following platforms, in what circumstances do you think the platform provider should be responsible for reimbursing them? Base: All U.S. respondents (2500)

American adults believe **full reimbursement** should be the top penalty for scams

Maximum punishment for scamming someone of their entire annual wage



Q27. Please imagine a scenario where the following punishments were passed for crimes in your country. What do you think the maximum punishment should be for scamming someone of their entire annual wage? Base: All U.S. respondents (2500)

Almost a third of American adults admit to committing **deceitful acts themselves**

Top 6 fraud types committed by American consumers



Q28. Which, if any, of the following have you done? Base: All U.S. respondents (2500)

31%

Of **American** adults admit to committing acts deemed as fraudulent



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 grow faster and more sophisticated, there is a global need for decisive action.

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.



Powered by Generali

Iris® Powered by Generali is a B2B2C global identity and cyber protection company owned by the 190-year-old multinational insurance company, Generali, that is passionate about not just developing effective identity protection solutions but also integrating them into people's lives in a meaningful and impactful way.

Today, we partner with some of the world's most well-known brands, protecting their people how they want to be protected, no matter where they are.

To learn more, visit IrisIdentityProtection.com



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 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 | 26th February – 14th 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). $\$1086.7 * 59612576 = 64780986171.4135$ (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

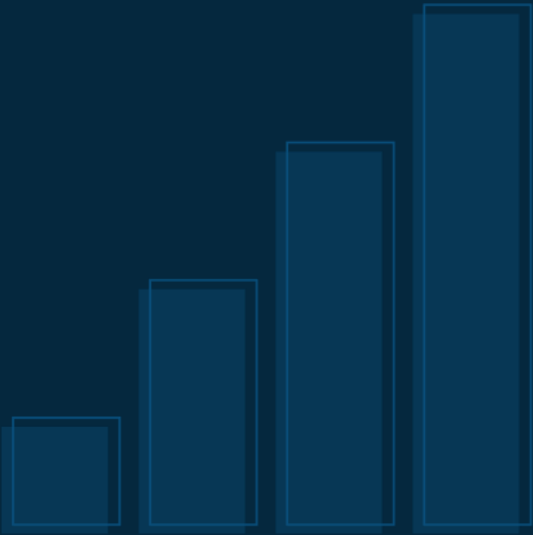


Our Foundation Members



Our Corporate Members





APPENDIX



Romance scams are the scam type mostly likely to last for longer than a day amongst Americans

Length of scam – by scam type

									Key =	Under index vs average	Over index vs average	
	Average (across scam types)	Investment	Shopping	Employment	Unexpected money	Impersonation	Charity	Romance / relationship	Fake invoice	Blackmail or extortion	Identity theft	Money recover
Minutes	44%	35%	37%	32%	38%	36%	33%	31%	43%	30%	38%	33%
Hours	16%	20%	19%	21%	19%	20%	22%	21%	17%	23%	19%	22%
Days	17%	21%	21%	23%	20%	22%	22%	24%	18%	22%	19%	21%
Weeks	8%	12%	10%	11%	10%	10%	10%	12%	9%	12%	9%	11%
Months	5%	5%	5%	5%	5%	5%	6%	6%	5%	5%	5%	6%
About a year	1%	2%	2%	2%	2%	2%	2%	3%	1%	3%	2%	2%
More than a year	1%	1%	1%	1%	1%	1%	1%	1%	1%	1%	2%	1%

Banks and payment providers are at the top of all aspects of preventing and resolving scams

Organisational ratings for aspects of preventing & resolving scams – 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
Responsibility ranking	3 rd	6 th	4 th	7 th	1 st	2 nd	5 th	8 th
Scam education & awareness	30%	43%	34%	47%	32%	32%	57%	40%
Scam blocking / payment prevention	32%	45%	29%	49%	33%	36%	58%	47%
Ease of scam reporting	32%	42%	30%	45%	40%	36%	62%	45%
Victim support / helpdesk	35%	50%	30%	46%	30%	34%	62%	33%
Scammer investigation / arrest	30%	47%	27%	44%	29%	29%	57%	38%
Reimbursement / compensation	27%	46%	26%	47%	28%	30%	65%	36%
U.S. ranking across all aspects	7 th	3 rd	8 th	2 nd	6 th	5 th	1 st	4 th



Powered by Generali



DISCLAIMER

This report is a publication by the Global Anti-Scam Alliance (GASA) supported by Iris® Powered by Generali. 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)

Global Anti-Scam Alliance (GASA)



Oder 20 – UNIT A6311
2491 DC The Hague
The Netherlands



General & Press Inquiries: partner@gasa.org



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



LinkedIn: linkedin.com/company/global-anti-scam-alliance