The 2024 State of Scams in the United Kingdom report, an annual study conducted by the Global Anti-Scam Alliance (GASA) and Cifas, highlights both encouraging trends and persistent challenges in the battle against scams in the UK. Based on responses from 2,000 Britons, we revisit the nation to shed light on the threats facing the public, and the emerging opportunities to counter those who deceive and defraud.

Britons are growing more confident in their ability to recognize scams, with 71% now reporting this confidence, a modest 2% increase from the previous year. Encouragingly, only 6% of respondents expressed a lack of confidence in identifying scams, suggesting that public awareness efforts are having a positive impact.

Despite increased awareness, 61% of Britons still encounter scams at least once a month, a slight 1% decrease since 2023. Alarmingly, over half (52%) of respondents reported experiencing more scam encounters over the past 12 months, indicating that scammers continue to find new ways to target potential victims. Notably, the use of artificial intelligence by scammers is widely recognized, particularly for generating text and images, although awareness of more advanced AI uses, such as voice and video manipulation, is lower.

The most common methods of scam delivery remain emails and text/SMS messages, with an 8% increase in SMS scams since last year. Trusted platforms like Gmail, WhatsApp, and Facebook are frequently exploited, with Facebook scams seeing a worrying 12% rise. The continued prevalence of these scams underscores the need for more effective safeguards on popular digital channels.

The financial and emotional consequences of scams are significant. In total, Britons lost £11.4 billion (US$14.5 billion) to scams in 2024, equivalent to 0.4% of the nation's GDP. The average loss per victim was $1,818, and only 18% of those who lost money were able to recover their losses—a concerning 15% drop from 2023. The emotional impact is also severe, with 53% of victims reporting a strong emotional toll, a 7% increase from the previous year.

Furthermore, the majority of scams go unreported, with 71% of Britons choosing not to notify law enforcement, a 5% rise from last year. This suggests a growing distrust in the effectiveness of authorities to address these crimes, along with confusion about where to report scams and frustration with complex reporting processes. Most victims, however, were able to recognize on their own that they had been scammed, although others relied on banks or family and friends to point it out.

Shopping scams remain the most prevalent form of fraud in the UK, while investment scams have grown more common since 2023. Victims are often drawn in by offers that seem "too good to be true" or act hastily without thoroughly verifying the legitimacy of these deals. The scams typically exploit popular payment methods such as credit cards, bank transfers, PayPal, and e-wallets, making it challenging for victims to recover their funds once taken.

The British public's trust in the internet has been deeply affected by scams, with 60% expressing a decline in trust. The general sentiment towards the government's efforts to combat scammers remains mixed, with 32% of respondents rating these efforts as very poor, while 34% viewed them favourably.

Despite the bleak findings, there is still hope. Nearly half of those surveyed follow the "if it is too good to be true, it probably is" rule, and many are proactive in checking for spelling errors and reviews to determine the legitimacy of an offer. Nevertheless, the persistence of scammers highlights the urgent need for better public education and enhanced anti-scam measures.

In conclusion, the people of the United Kingdom need more support from their government, law enforcement, and financial institutions. The staggering loss of £11.4 billion to scams demands action—public education campaigns, streamlined reporting processes, and an unwavering commitment to bringing scammers to justice. The fight against scams must be intensified to restore confidence and protect citizens from the growing threat of fraud.

Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

# Developments will help disrupt and prevent some scams, but much more needs to be done as the UK fights back

The UK is facing a scams emergency that is showing no signs of slowing down as criminals adapt, evolve, and intensify the ways in which they target UK consumers and business.

In 2023, research Cifas co-commissioned with the Global Anti-Scam Alliance (GASA), revealed that UK consumers lost £7.5 billion to scams, and 1 in 10 people were targeted by these callous criminals.

Since then, changes in technology have enabled more targeted phishing tactics, and with the ease and accessibility of AI tools, even the most novice of criminals can become sophisticated scammers.

Social media and other online platforms also continue to provide a rich seam of opportunities for criminals. And scammers are not only stealing victims' money, but their identities too – adding to the worry, shame, and blame many people feel after they have been scammed.

The truth is that anyone can be a victim of a scam, and as this research sets out, most of us are lucky not to have been. Scammers tap into trends and world events, reacting quickly to of-the-moment news to exploit our vulnerabilities. Scams include fake Black Friday deals and concert tickets, and spoofed car finance refunds and tax rebates. Most scammers act quickly to avoid detection – using automation, chatbots, and different online channels to move from one target to the next with ease.

The relentless nature of scamming only underpins just how important the challenge is that we all face as a fraud prevention community.

However, there are signs that the UK is fighting back.

In 2024, we have seen a new Government come to power and the appointment of a Fraud Minister for the first time, Lord Hanson. This is a welcome step. It's vital for effective fraud prevention that we have real political leadership – someone who is passionate about rooting out the problems, protecting the public and business, and bringing criminals to justice.

Additionally, the Payment Systems Regulator has introduced new rules that mandate Payment Service Providers (PSPs) to reimburse the victims of Authorised Push Payment (APP) fraud 50:50. While this reform is clearly well-intentioned, introducing much needed and consistent protections for consumers, and helping to incentivise new investment in fraud prevention tools, we need to be on our guard to ensure the refund scheme is not abused.

At Cifas, we have long been campaigning to better protect consumers from fraud and online scams. Our Fraud Pledges, launched in May 2024, called for the Government to do more to help keep people and businesses safe, this includes ensuring big tech and online platforms play a full role in efforts to tackle fraud and scams.

As the UK's leading fraud prevention service, we have made significant investment in the development of new products and services to help organisations respond to the ever-evolving tactics of scammers.

In 2023, we helped our 750-plus membership prevent £1.8 billion in fraud losses, launching new fraud prevention tools and services including our APP Victim Check and Beneficiary Checking Service. Along with Get Safe Online, we supported the 'Check a Website' initiative – a UK extension of ScamAdviser.com developed by GASA which helps consumers verify URLs and spot scam attempts.

Throughout the community, exciting innovations – such as Virgin Media O2's 'AI Daisy' designed to waste scammers' time on the phone – continue to show the UK's strength not just in fraud prevention, but efforts to dismantle organised crime groups and disarm scam centres through public-private partnership and technical innovation.

However, while these developments will help disrupt and prevent some scams, much more needs to be done.

With greater collaboration through stepping up the sharing of data and intelligence across the entire fraud lifecycle, we can turn the tide on scams – both in the UK and globally.

It has been a privilege to work together with GASA to bring you this important research. I am sure you'll find it valuable. I also hope, like me, it is a salient reminder of the necessity of working together to stop scammers at source.

Mike Haley
CEO

# 2,000 Britons completed the State of Scams survey

## Gender



45%    55%

## Age Range

18-24
25-34
35-44
45-54
54+

0    10    20    30    40

## Education

35%
30%
25%
20%
15%
10%
5%
0%

middle school    high school    vocational    university    postgraduate
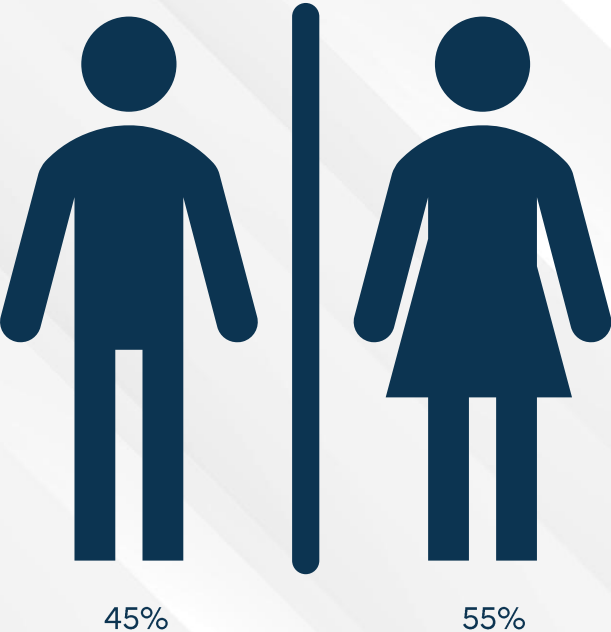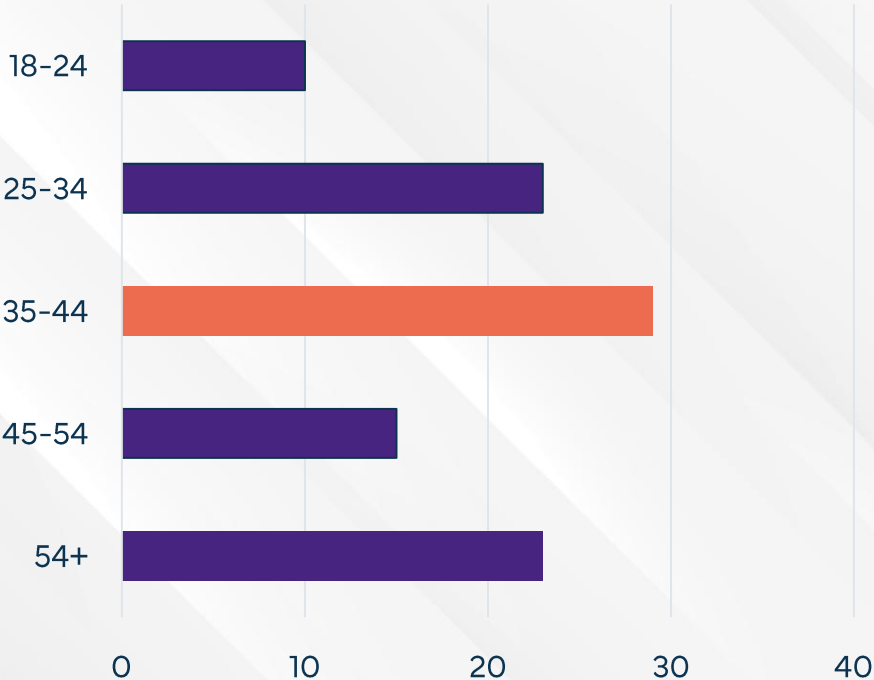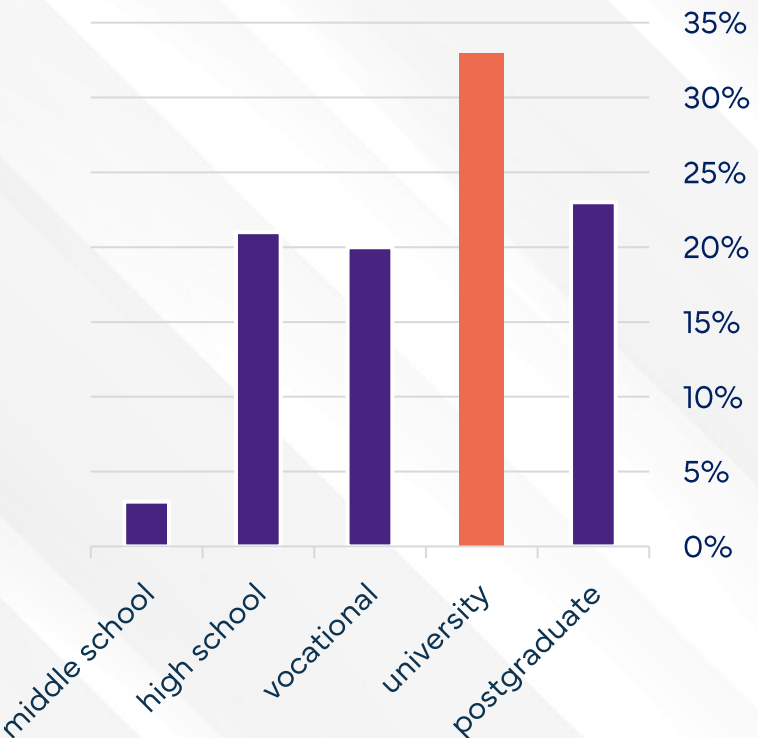
The demography of respondents to the State of Scams in the United Kingdom 2024 survey consists of more women than men. A large proportion were between 35-44 of age, with university degree.

# 71% of Britons are confident in their ability to recognise scams



Respondents (%)

**2%** more confident in recognizing scams versus 2023

Very Confident — Not Confident at all
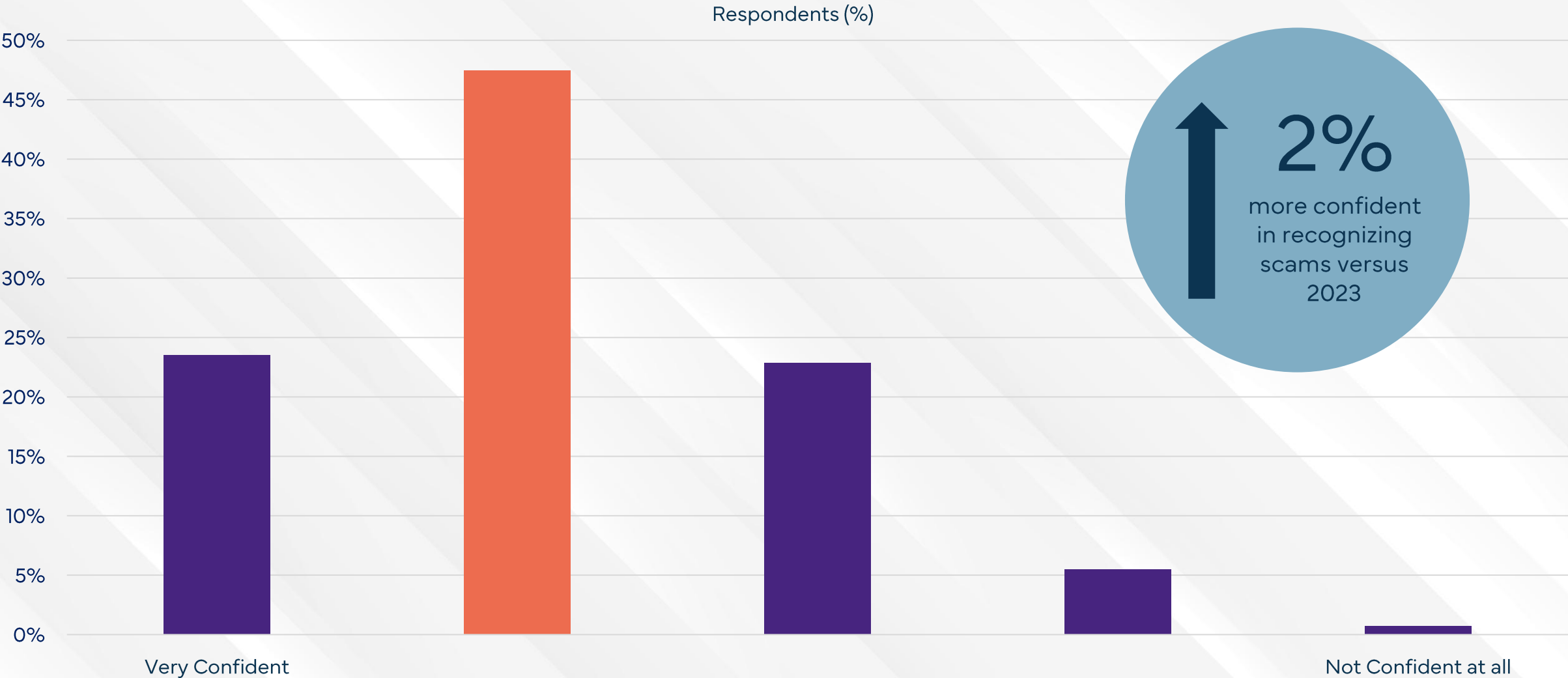
Only 6% of respondents are not (very) confident in recognising scams, at all.

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

# 61% of Britons encounter scams at least once per month

**Cifas** Fighting Economic Crime Together

**GASA** Global Anti-Scam Alliance

Respondents (%)



↓ **1%** fewer scams encountered per month, since 2023

| Category | |
|---|---|
| Every day | |
| Several days per week | |
| Once a week | |
| Once a month | |
| About every few months | |
| Once a year | |
| Less often | |
| Never | |

0%  5%  10%  15%  20%  25%  30%
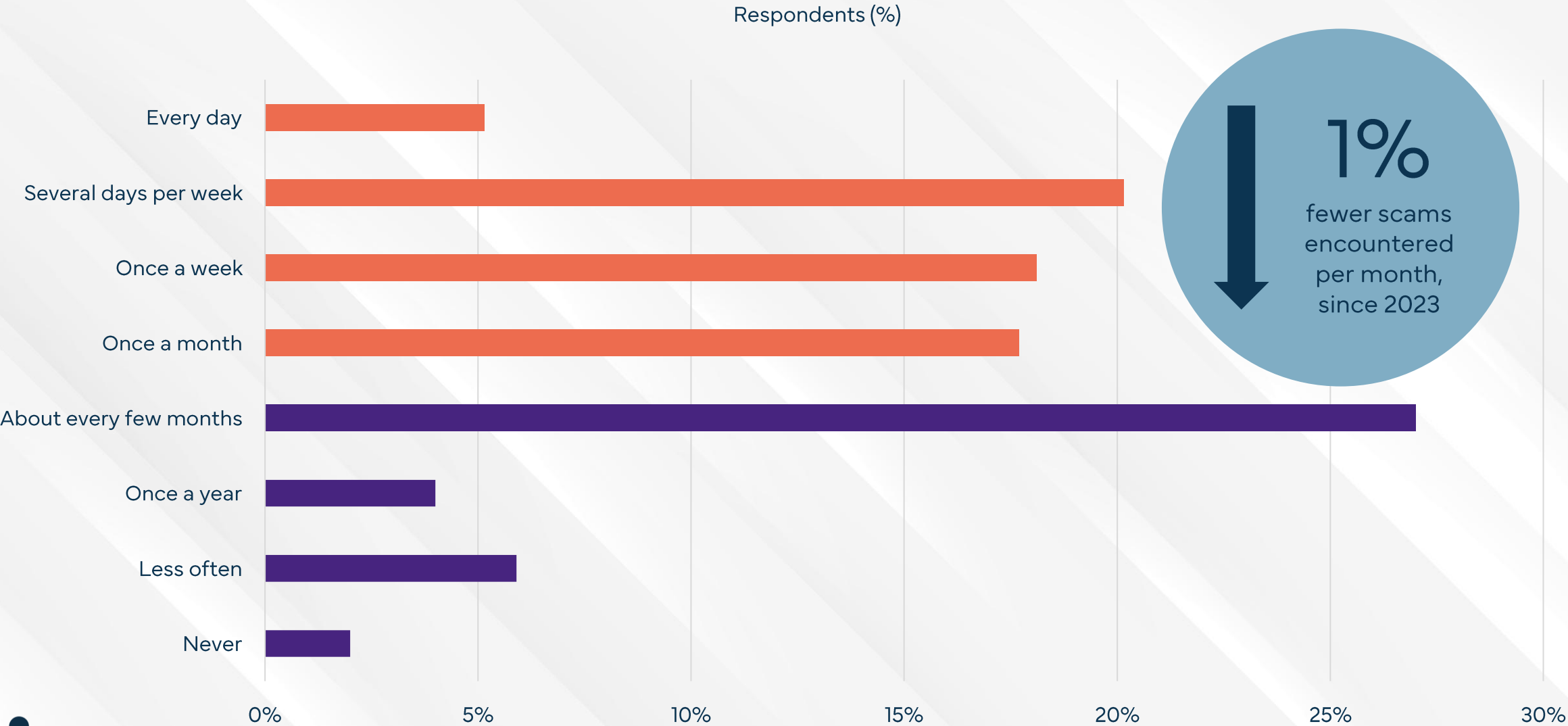
**6% of British respondents encountered fewer scams this year, compared to the previous 12 months.**

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

# 52% of Britons faced more scam encounters over the last 12 months

CIFAS
Fighting Economic Crime Together

GASA
Global Anti-Scam Alliance

Respondents (%)



**12%**
saw a reduction in scam encounters over 12 months

Significantly more

Same

Significantly less

0%    10%    20%    30%    40%    50%    60%
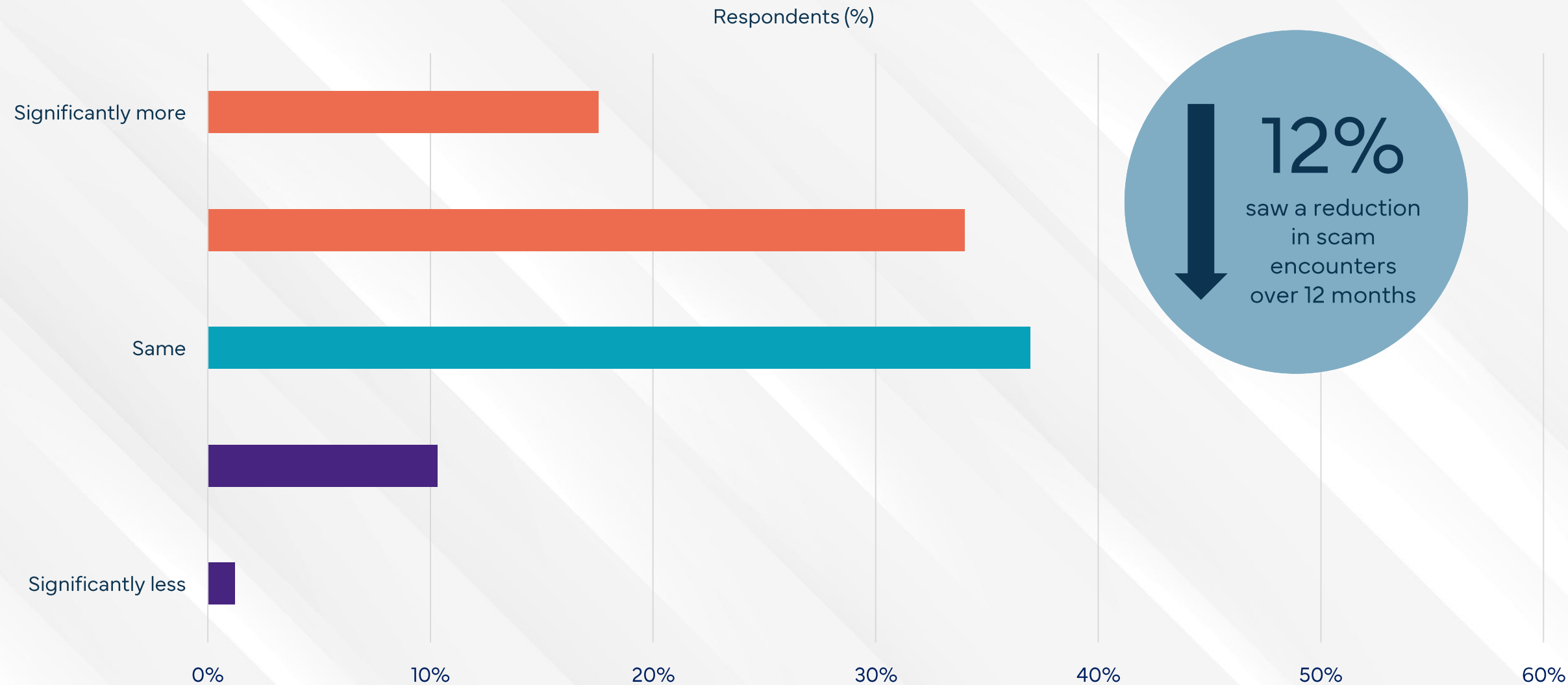
**37% of British respondents experienced similar number of scam encounters in the past 12 months.**

Q4 – Compared to the year before, do you feel you have been exposed more or less frequently by an individual/company that tried to deceive you in the last 12 months?

# Most Britons are aware scammers can use AI against them



Respondents (%)
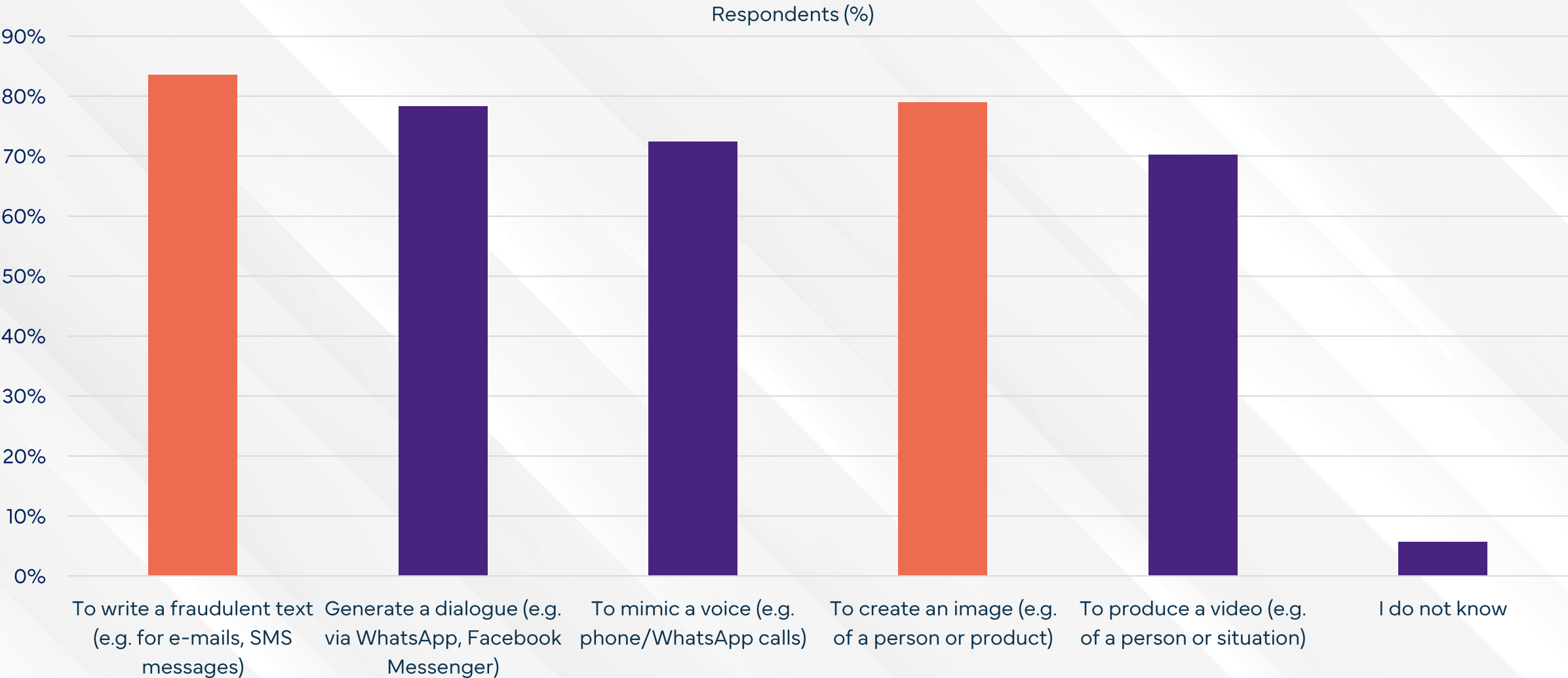
Awareness of AI generated text & images is high, while complex AI voices & videos are less widely known.

Q5 – For which of the following can Artificial Intelligence (AI) be used?
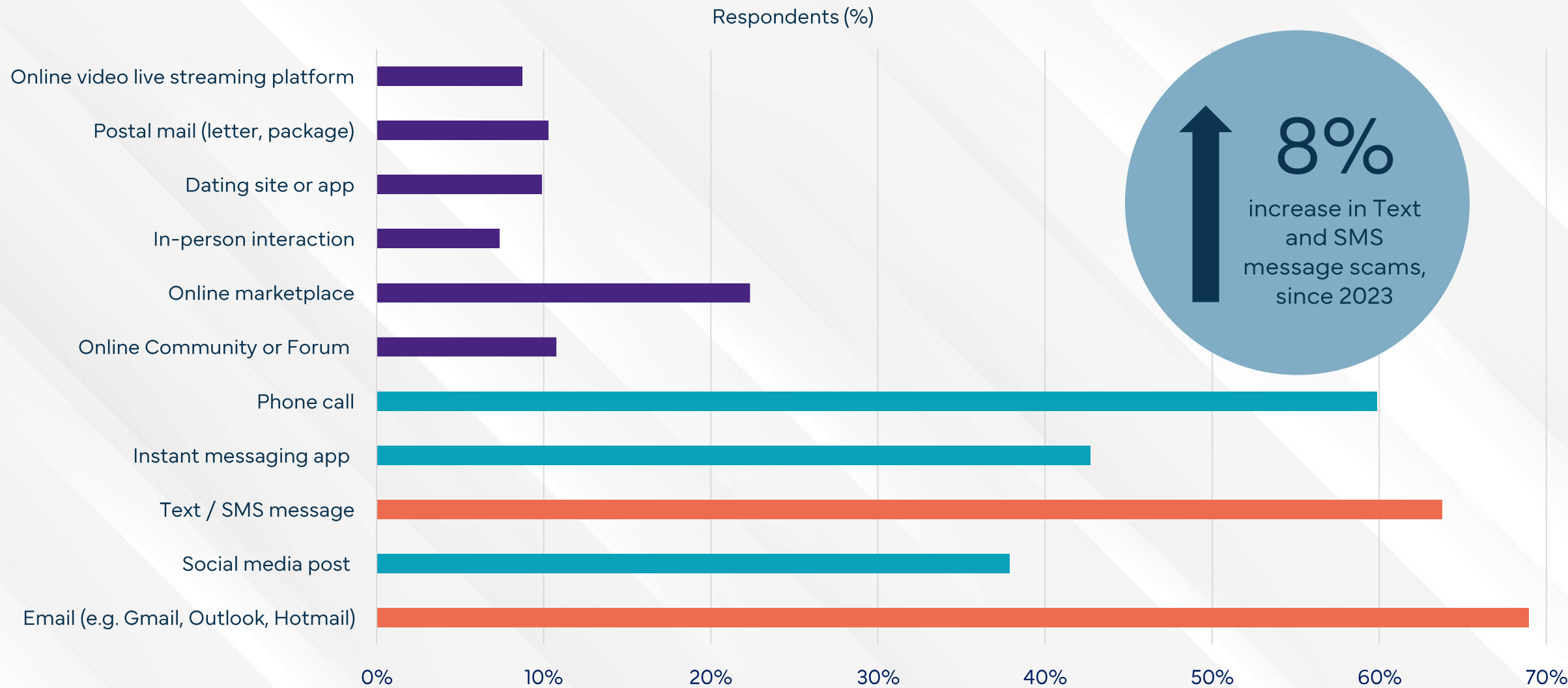
# Gmail, WhatsApp & Facebook are the most exploited platforms



Respondents (%)

**12%** ↑ Facebook scams have continued to rise since 2023
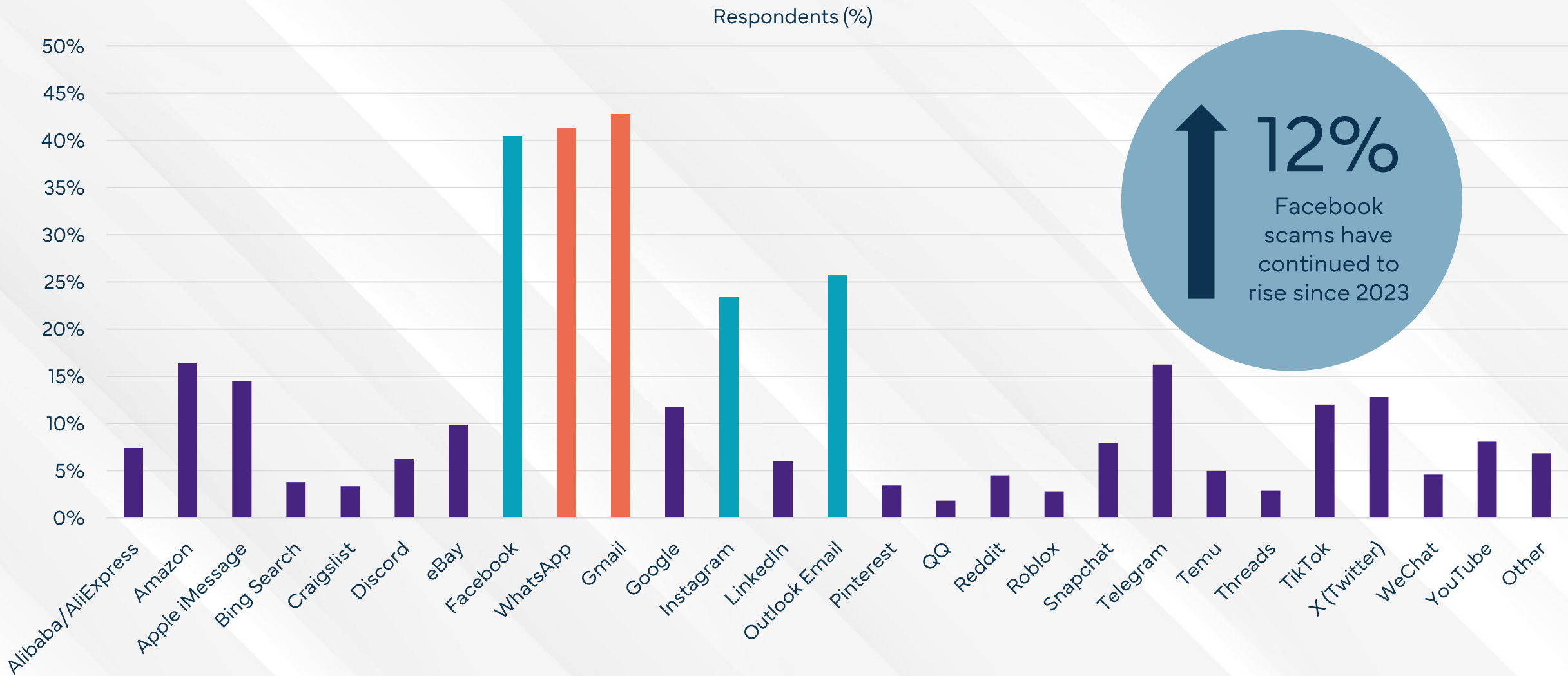
## Outlook Email & Instagram round out the top five platforms where people encounter scams.

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

# 71% of Britons did not report the scam to law enforcement

CIFAS
Fighting Economic Crime Together

GASA
Global Anti-Scam Alliance

Don't Know, 1%

Yes, 28%

No, 71%

↑ 5%
more Britons are not reporting scams to law enforcement
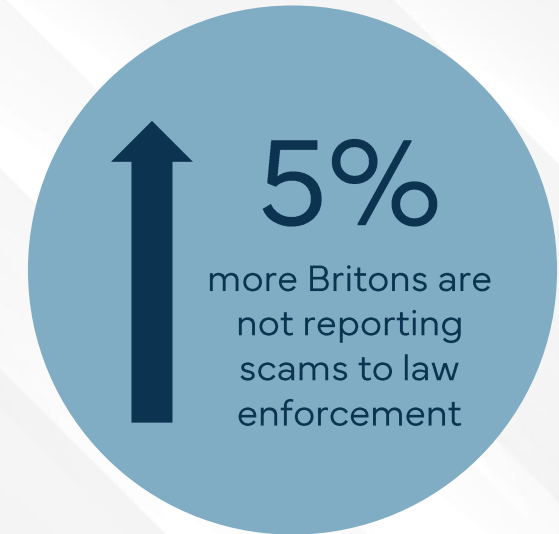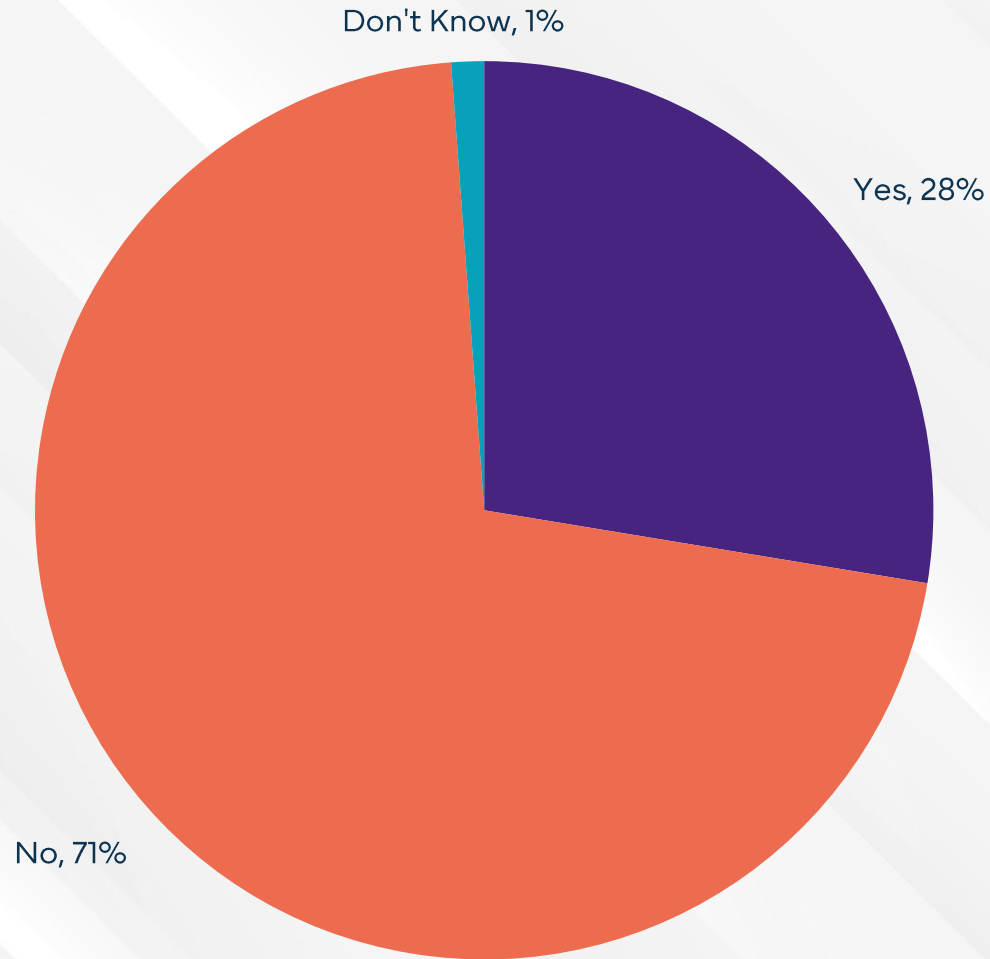
28% stated having reported the scam to law enforcement or another government authority.

Q8 – Did you report a scam or scam attempt to the police or authorities in the last 12 months?

# 44% of Britons were uncertain whether AI was used to scam them

CIFAS
Fighting Economic Crime Together

GASA
Global Anti-Scam Alliance

Respondents (%)

| Category | |
|---|---|
| Yes, in a text message I received | |
| Yes, in a chat conversation I've had | |
| Yes, in a voice call I received | |
| Yes, in a picture I received | |
| Yes, in a video I received | |
| Maybe, I don't know | |
| No, I have not received a scam message created by Artificial Intelligence | |

0%   5%   10%   15%   20%   25%   30%   35%   40%   45%   50%
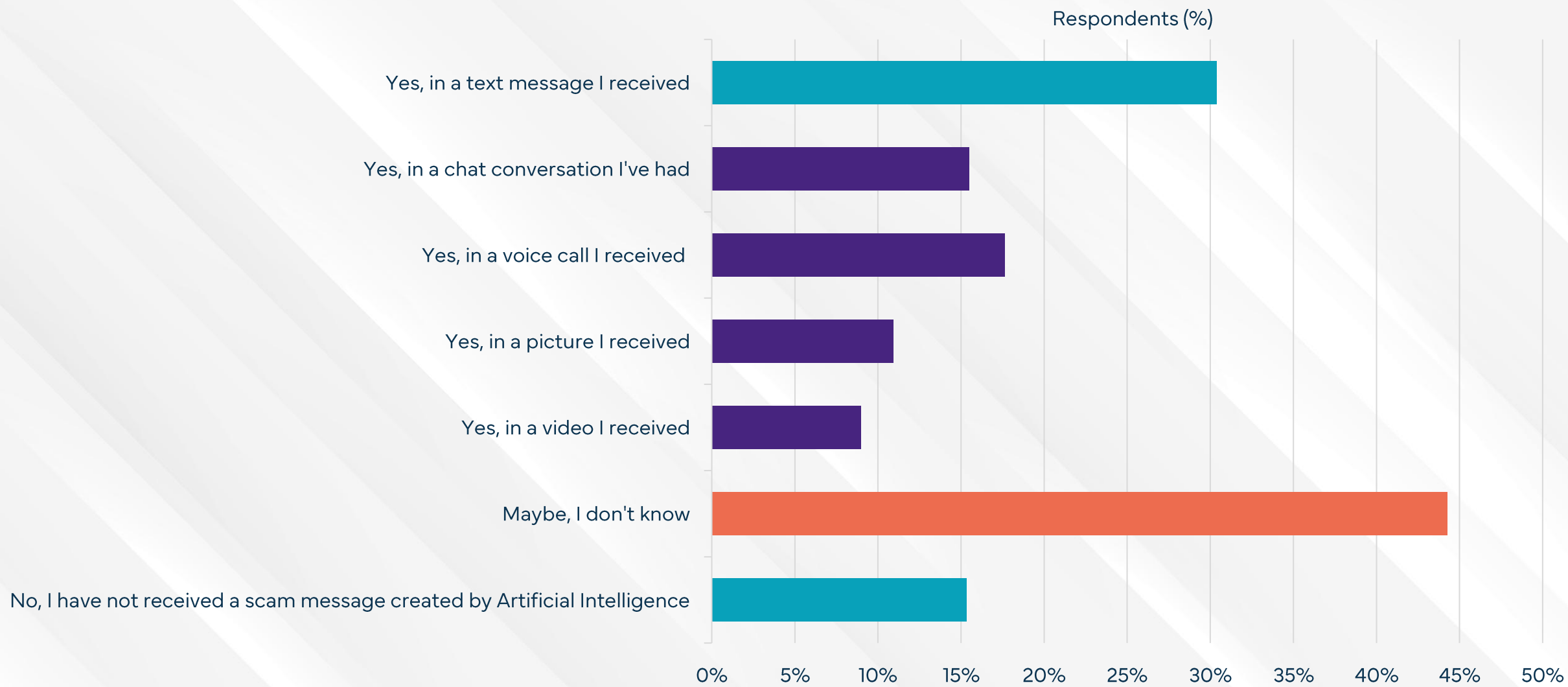
**15% of Britons stated they did not believe they were subjected to scams utilizing artificial intelligence.**

Q9 – Do you think Artificial Intelligence (AI) was used in an attempt to scam you?

# Shopping Scams are the most common type of scam in the UK

**CIFAS** — Fighting Economic Crime Together
**GASA** — Global Anti-Scam Alliance

Respondents (%)

| Scam type | Approximate value |
|---|---|
| Investment | ~12.5% |
| Shopping | ~19.5% |
| Employment | ~9.5% |
| Advance Fee | ~10% |
| Authority | ~8.5% |
| Charity | ~11.5% |
| Romance / Friend in Need | ~10% |
| Fake Invoice / Debt | ~6.5% |
| Threats & Extortion | ~6% |
| Identity theft | ~18.5% |
| Other | ~2% |

0%   5%   10%   15%   20%   25%   30%

**↑ 5%** investment scams became more common, since 2023

"I gave personal information to somebody that phoned me."

**50% did not fall victim to the most common scams in the last year. 1.15 scams were reported per victim.**

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

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

"I was promised 100% return on investment which failed."

"I was buying Jordan 4s for cheaper on Instagram as a I saw multiple good reviews and they were real and not replicas however mine never came and I texted and emailed on everything but I still didn't receive them and I bought them for nearly £300."

"Received alert from bank for a transaction that wasn't mine. No idea how my card details were exposed."

# 49% of scams are completed within 24 hours of first contact

Respondents (%)
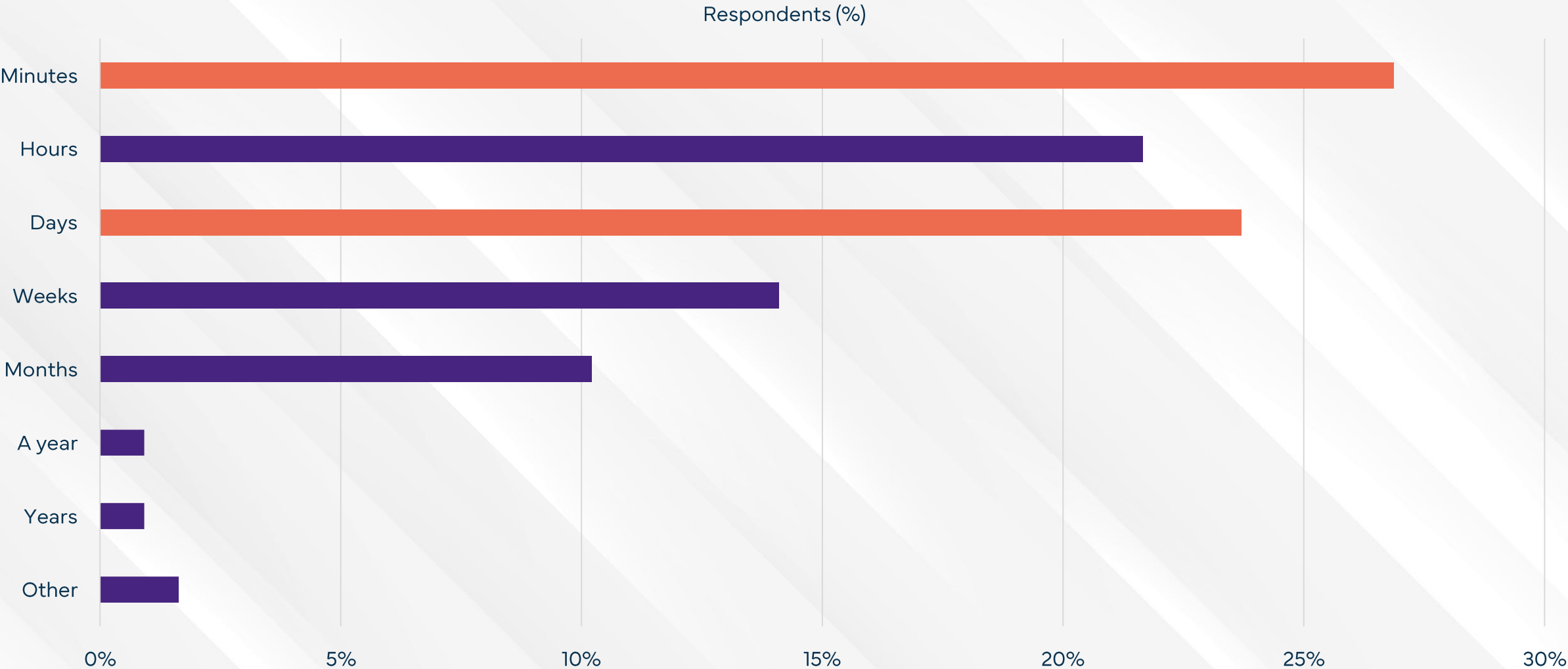
27% reported scams that were over in minutes, while 2% were scammed over a year or more.

Q12 - How long did the scam last, from the first time you heard from the scammer until the last payment you made or the last time you contacted them?

# Nearly half the victims realized on their own they had been scammed

Respondents (%)
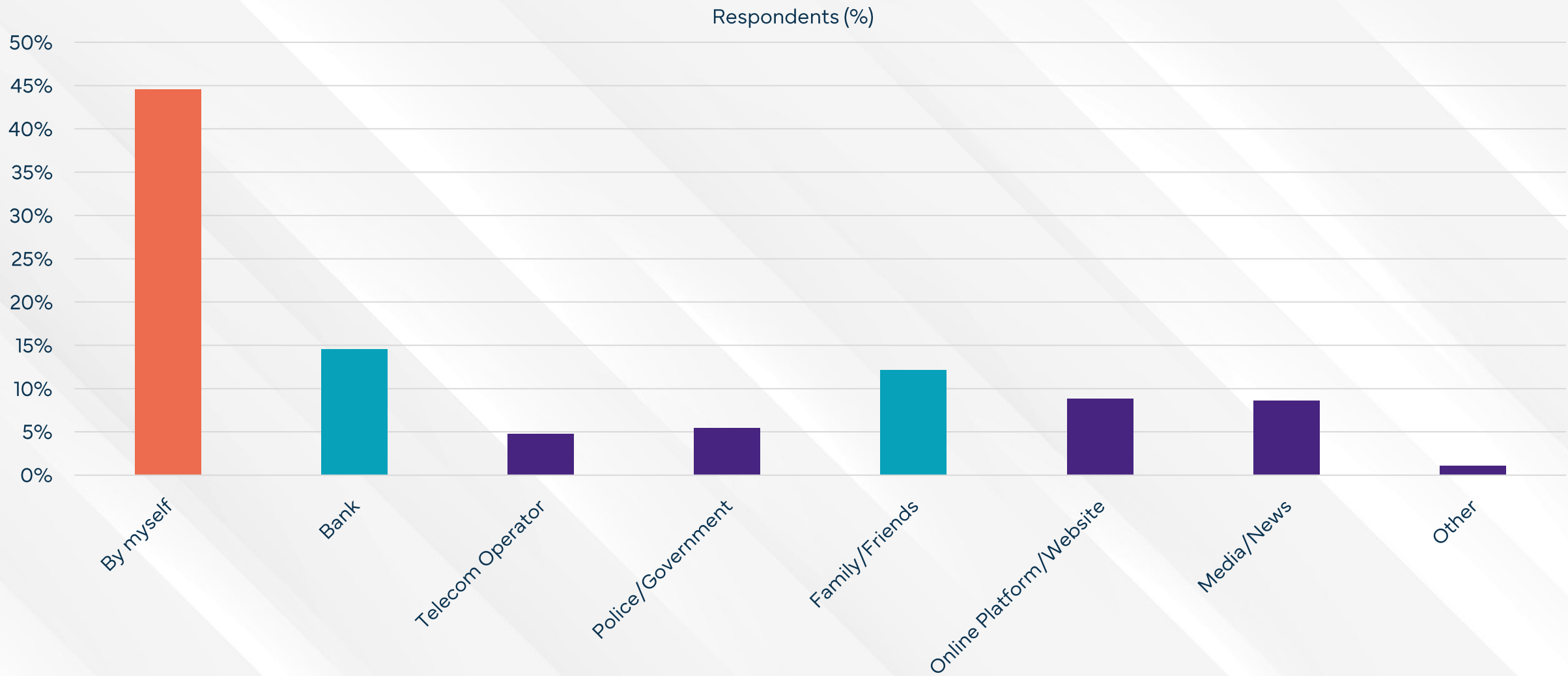


Others were informed by banks, while family/friends are also popular in pointing out scams.

Q13 - How did you discover you were scammed?

# In total, 15% of British participants lost money in a scam

## Survey Key Statistics

| | |
|---|---|
| Persons approached | 4,651 |
| Participants completing the survey | 43% |
| Participants losing money | 681 |
| % losing money / approached persons | 15% |
| Average amount lost in US Dollars | 1,818 |
| Total country population | 68,459,055 |
| Population over 18 years | 54,572,588 |
| # of people scammed > 18 years | 7,990,245 |
| Total scam losses (USD) | 14,526,266,268 |
| Total scam losses (GBP) | 11,394,358,263 |
| Gross Domestic Product (USD, millions) | 3,332,059 |
| % of GDP lost in scams | 0.4% |

Respondents (%)
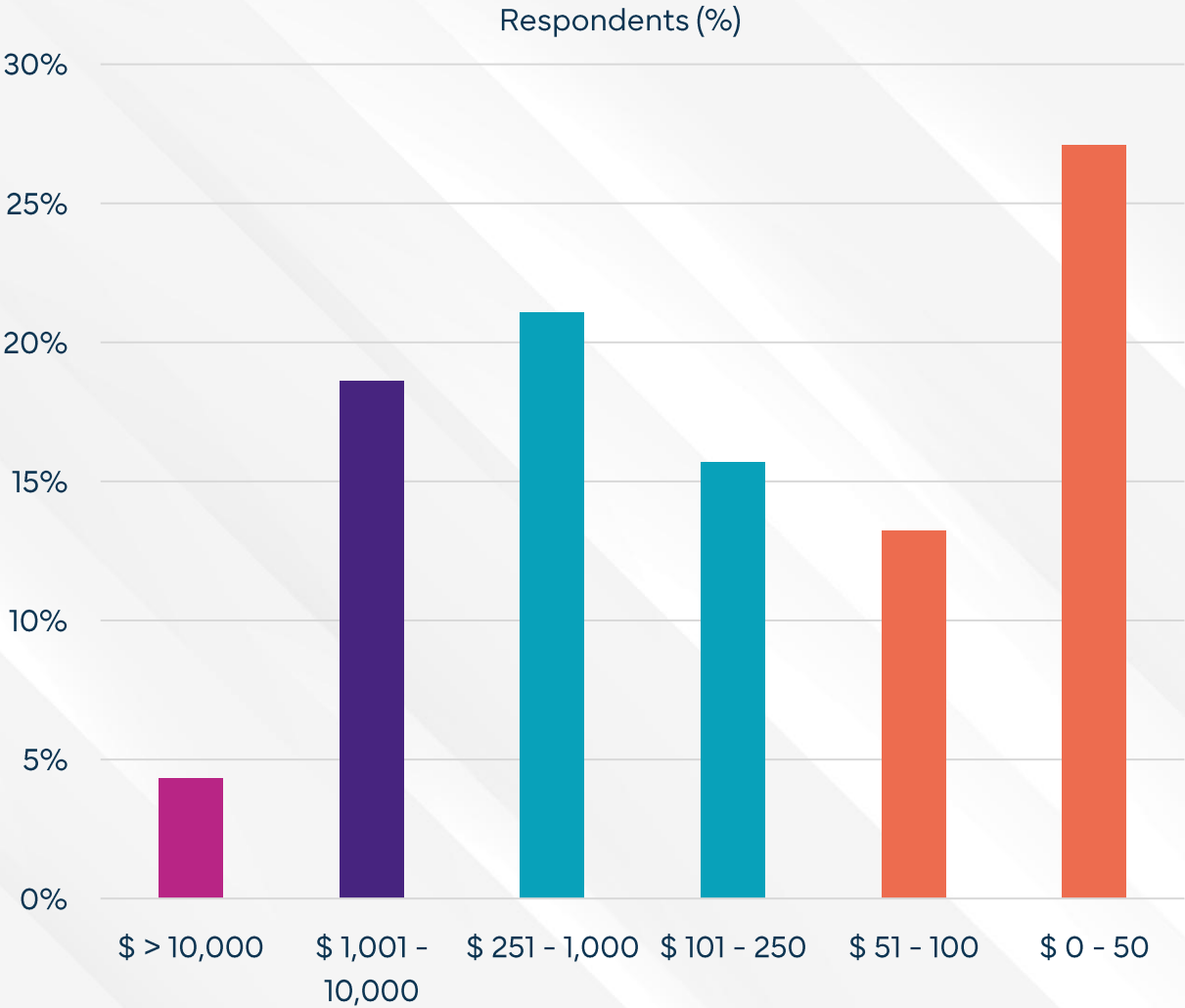


In total, the British lost £11.4 billion to scams, which is equal to 0.4% of the United Kingdom's GDP.

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

# Credit Cards & Bank Transfers are the dominant payment methods

Respondents (%)



| Payment method | Approximate % |
|---|---|
| Cash / check | ~11% |
| Electronic / bank transfer | ~31% |
| Gift cards (physical / digital) | ~15% |
| PayPal | ~28% |
| e-Wallet | ~16% |
| Credit card | ~46% |
| Peer-to-peer online payment | ~13.5% |
| Cryptocurrency transfer | ~16% |
| Via another payment method | ~1.5% |

0%  5%  10%  15%  20%  25%  30%  35%  40%  45%  50%
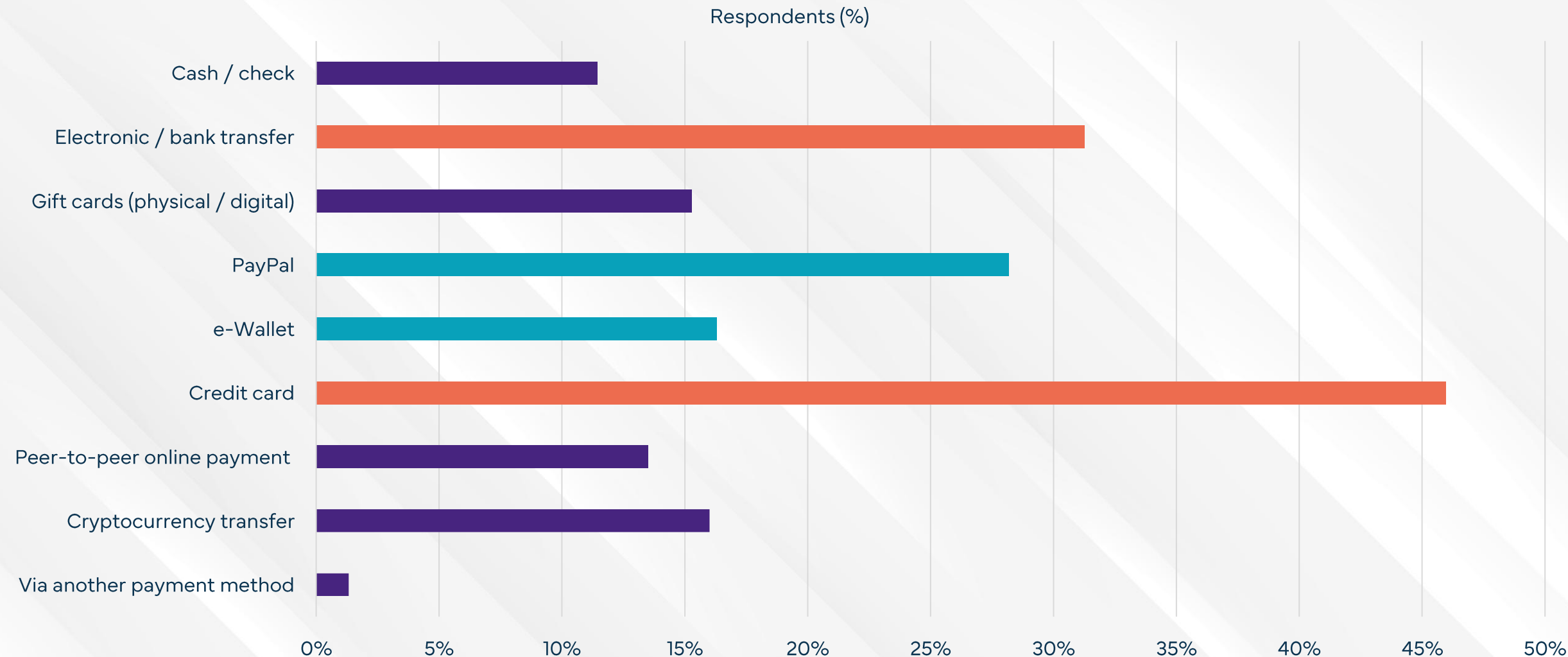
**PayPal and e-wallets are also popular tools which scammers use to receive their stolen gains.**

Q15 - How did you pay the scammer?

# Only 18% of victims were able to fully recover their losses



Respondents (%)

- Yes, I got all the money back
- Yes, I got a large part of the money back
- Yes, but I only got a small part of the money back
- Yes, but I didn't get any money back
- No, I didn't try

15% drop in victims fully recovering their losses, since 2023
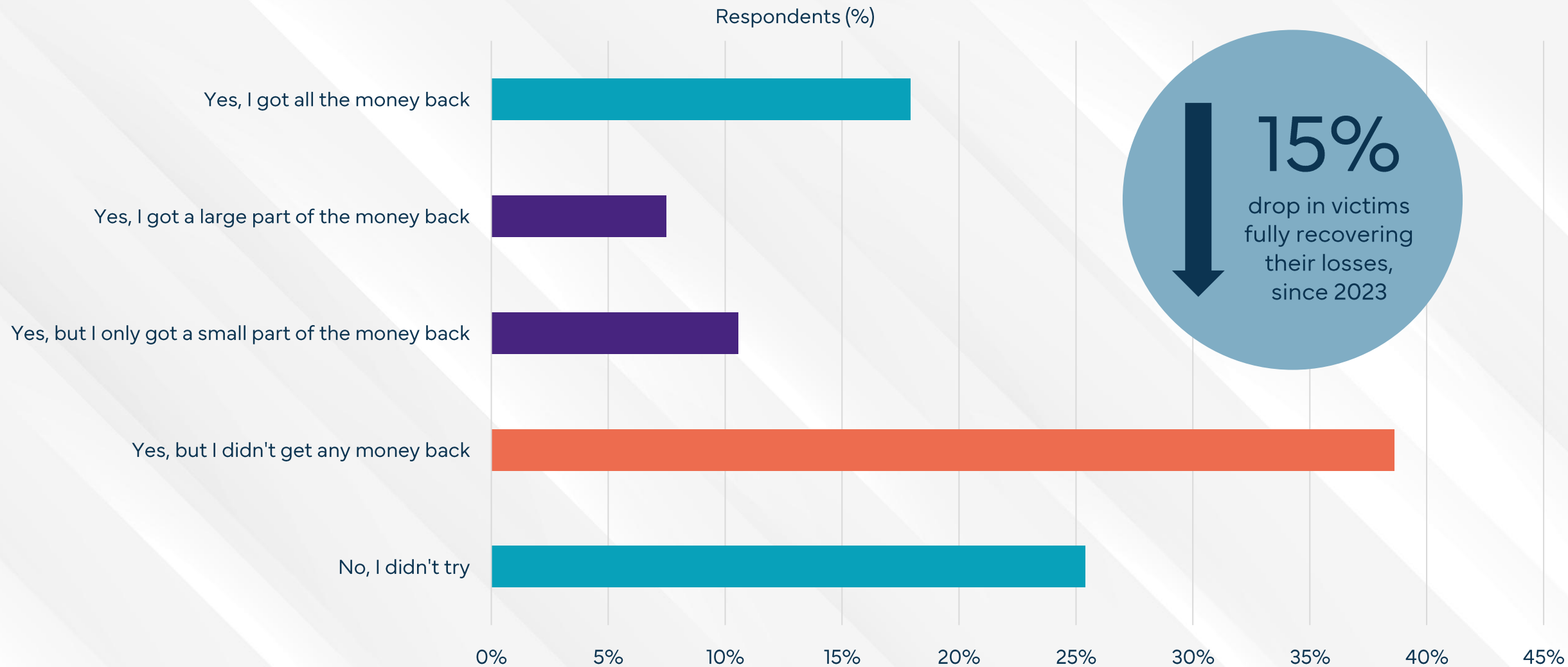
**25% did not try to recover their funds. 39% tried but were not able to recover any money.**

Q16 – Did you try to recover the money lost?

# 53% of the scam victims perceived a (very) strong emotional impact

Respondents (%)



↑ **7%** rise in heavy emotional impacts, since 2023

Maximum impact          Moderate          No impact
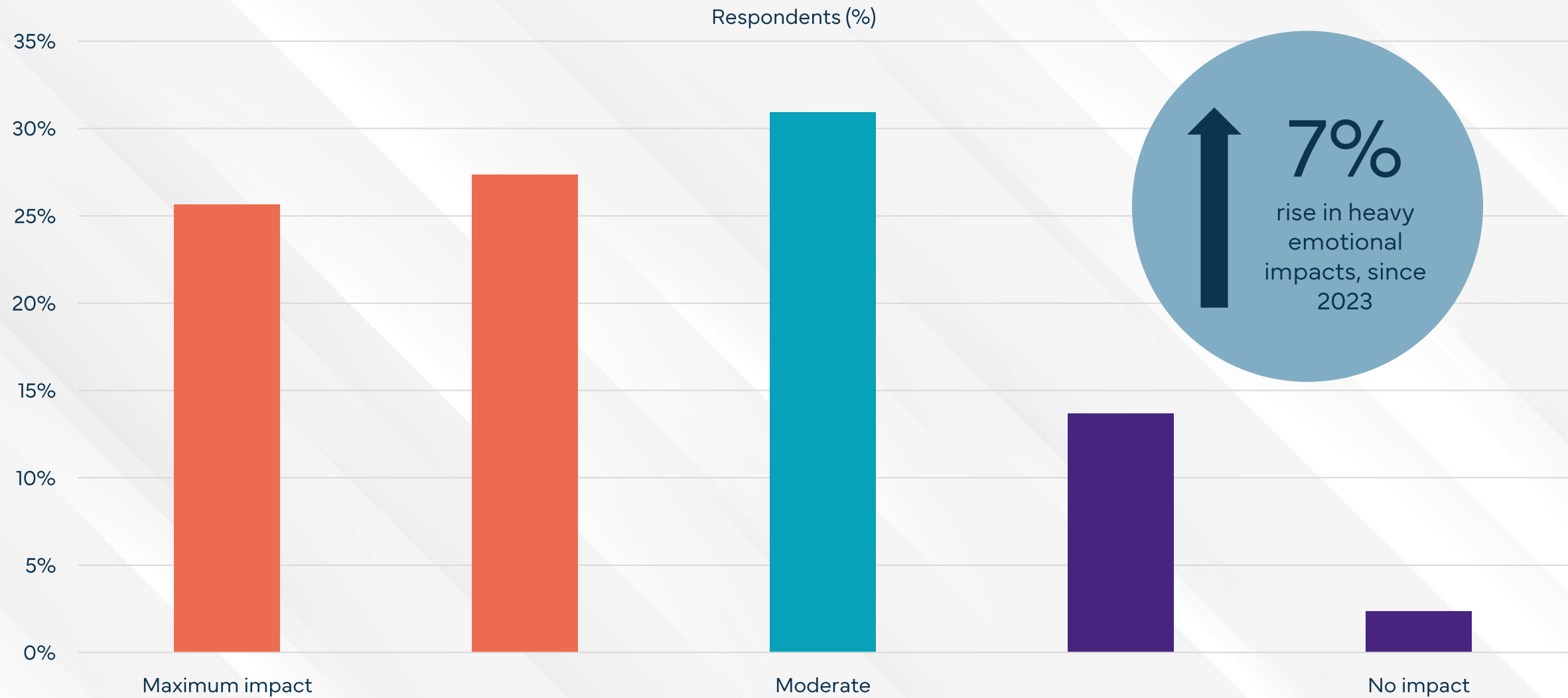
**16% of the survey respondents reported little to no emotional impact due to scams.**

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

# 60% of Britons have less trust in the Internet as a result of scams

Respondents (%)

| | |
|---|---|
| Maximum impact | |
| Moderate | |
| No impact | |

0%  5%  10%  15%  20%  25%  30%  35%
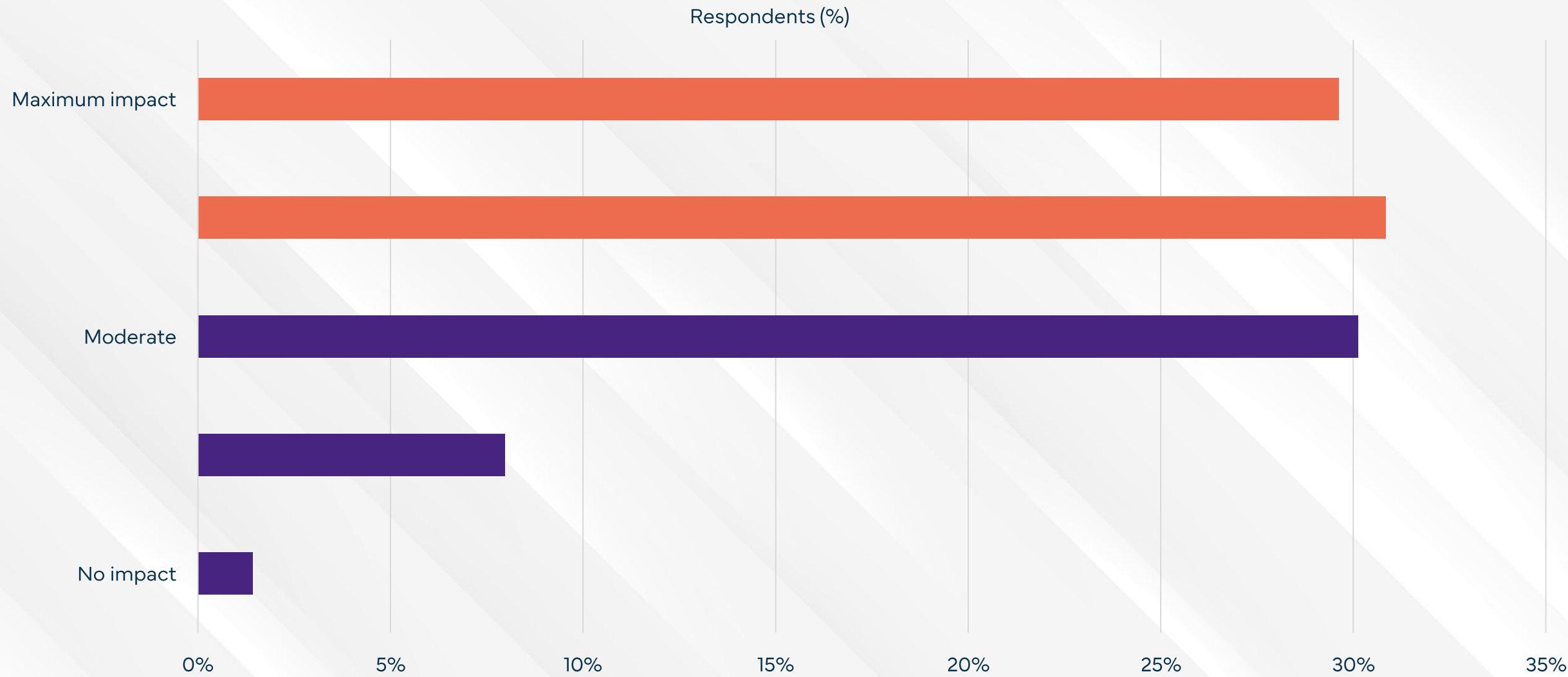
## Only 9% of Britons reported little to no loss of trust in the Internet due to scams.

Q18 – To what extend do scams impact your trust in the Internet, in general?

# Britons often fall for scams because the offer is so attractive

Respondents (%)

| Category | |
|---|---|
| I didn't see the scam | (~13%) |
| I acted very quickly | (~22%) |
| I did not have the knowledge to recognize the fraud | (~11%) |
| I was attracted by the offer I received | (~25%) |
| I wasn't sure if it was a scam but I chose to take a chance | (~8%) |
| I was forced to participate | (~4%) |
| I trusted a friend/family member | (~8.5%) |
| Other | (~2.5%) |
| None of the above | (~5%) |



"I was unaware of the scam until my bank (informed) me."
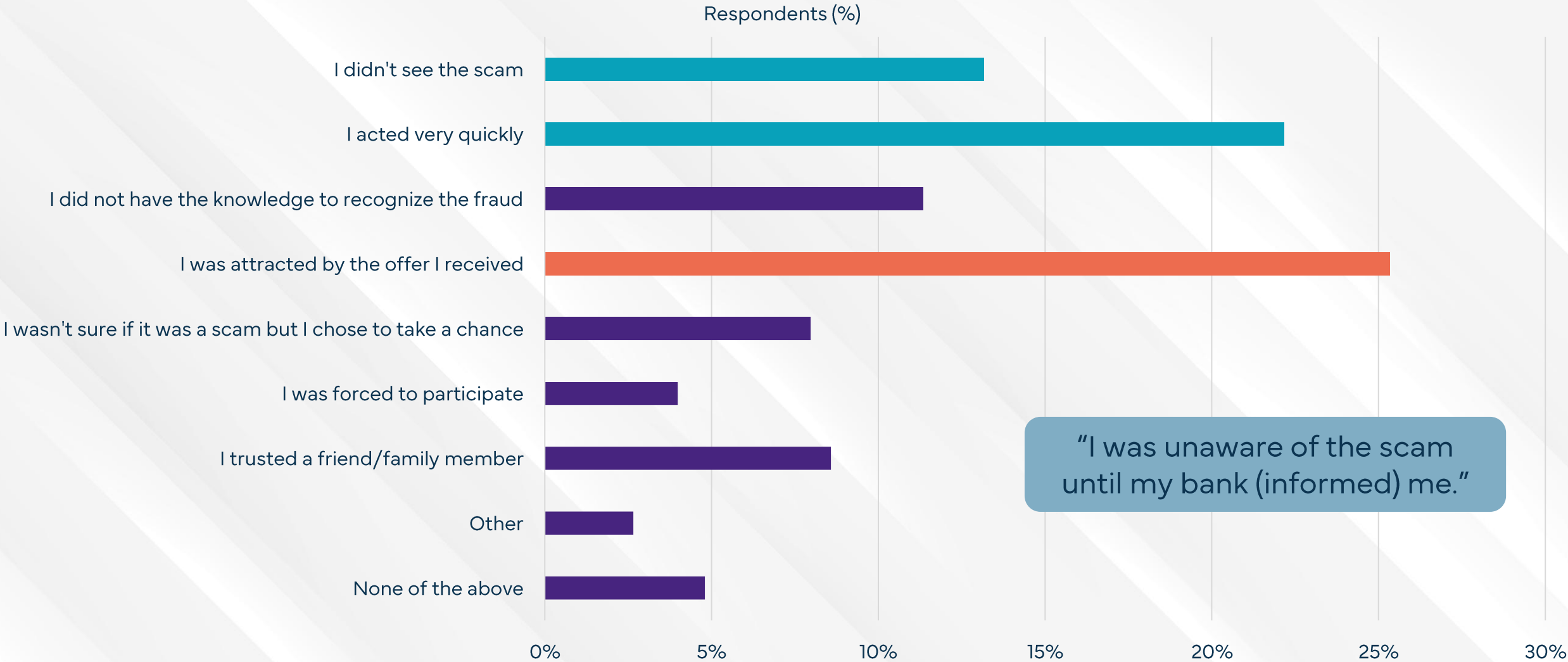
**Several victims also reported acting hastily while others were unable to see the scam.**

Q19 – What was the main reason you were deceived?

# Nearly half follow the "if it is too good to be true, it probably is" rule

Respondents (%)



| Step | Respondents (%) |
|---|---|
| I look for reviews on the same web page | ~27% |
| I ask friends or family | ~19% |
| I'll do a reverse image search to see if they show up elsewhere | ~13% |
| I check for copied text on the web page (plagiarism) | ~10% |
| I check for spelling and grammatical errors | ~46% |
| I check for the presence of a phone number | ~22% |
| I verify that the website has a valid SSL certificate | ~19% |
| I check if the payment can be made by a refundable payment method | ~21% |
| I follow the rule "if it seems too good to be true, it probably is" | ~48% |
| I look for reviews on other websites | ~37% |
| I check if the company is active on social media | ~21% |
| I call the person/company to check | ~16% |
| I check if the email address is from a free email provider (e.g. Gmail, Hotmail) | ~34% |
| I check if the phone number is an IP phone number (Internet) | ~17% |
| I check company registers (listed by Companies House) | ~18% |
| I am looking for a seal or other form of certification | ~16% |
| I used an anti-fraud app/website to check | ~17% |

## Many reported checking for spelling & grammatical errors and checking reviews on other websites.

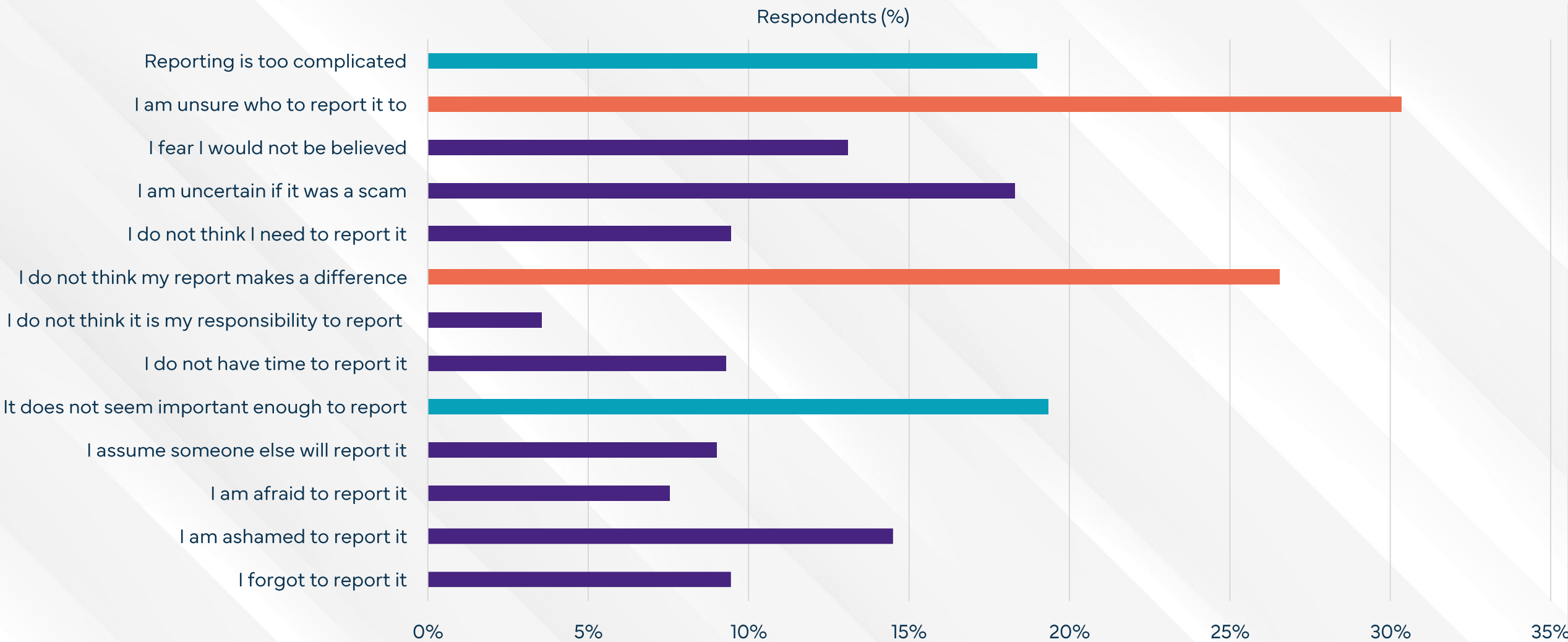Q20 – What steps do you take to check if an offer is real or a scam?

# Scams are mostly shared with banks & local law enforcement

**CIFAS** Fighting Economic Crime Together

**GASA** Global Anti-Scam Alliance

Respondents (%)

| Category | |
|---|---|
| National Reporting Website | |
| Local Police Department | |
| National Police Agency | |
| Consumer Protection Authority or Organization | |
| Family and Friends | |
| Online Review Site (e.g. Trustpilot, Google Reviews) | |
| Financial Protection Authority | |
| Social Media, Blogs or Forums | |
| Internet Service Provider or Hosting Company | |
| My Bank / Payment Provider | |
| My Telecom/Mobile Operator | |
| Anti-scam app/website | |
| I would not report the scam | |
| Other | |

0%    10%    20%    30%    40%    50%    60%

**Family & friends, anti-scam app/website & online review sites are popular places to report scams.**

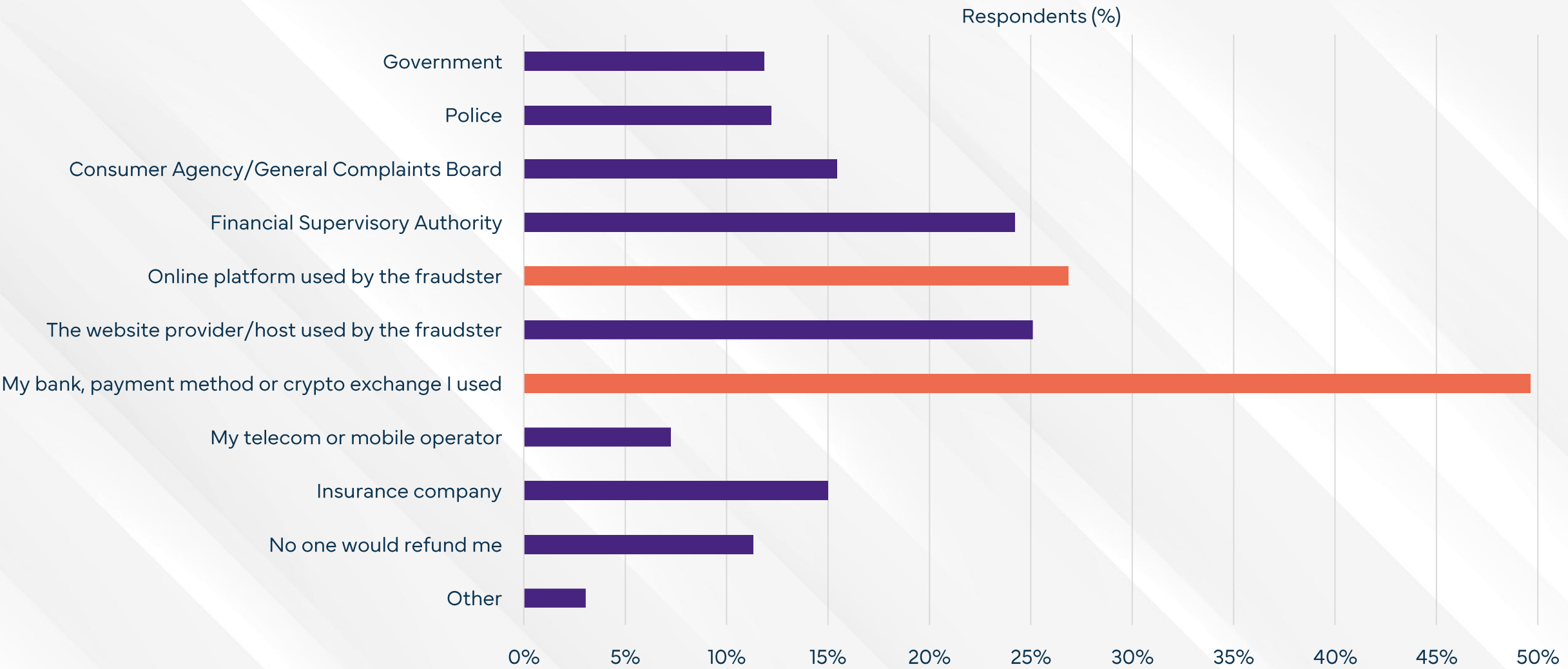Q21 - If you were to be deceived by a scam, who would you report this to?

# Many Britons are uncertain where to report scams



Respondents (%)

| Reason | |
|---|---|
| Reporting is too complicated | |
| I am unsure who to report it to | |
| I fear I would not be believed | |
| I am uncertain if it was a scam | |
| I do not think I need to report it | |
| I do not think my report makes a difference | |
| I do not think it is my responsibility to report | |
| I do not have time to report it | |
| It does not seem important enough to report | |
| I assume someone else will report it | |
| I am afraid to report it | |
| I am ashamed to report it | |
| I forgot to report it | |

## Other reasons for not reporting are assuming reporting isn't important and complex processes.

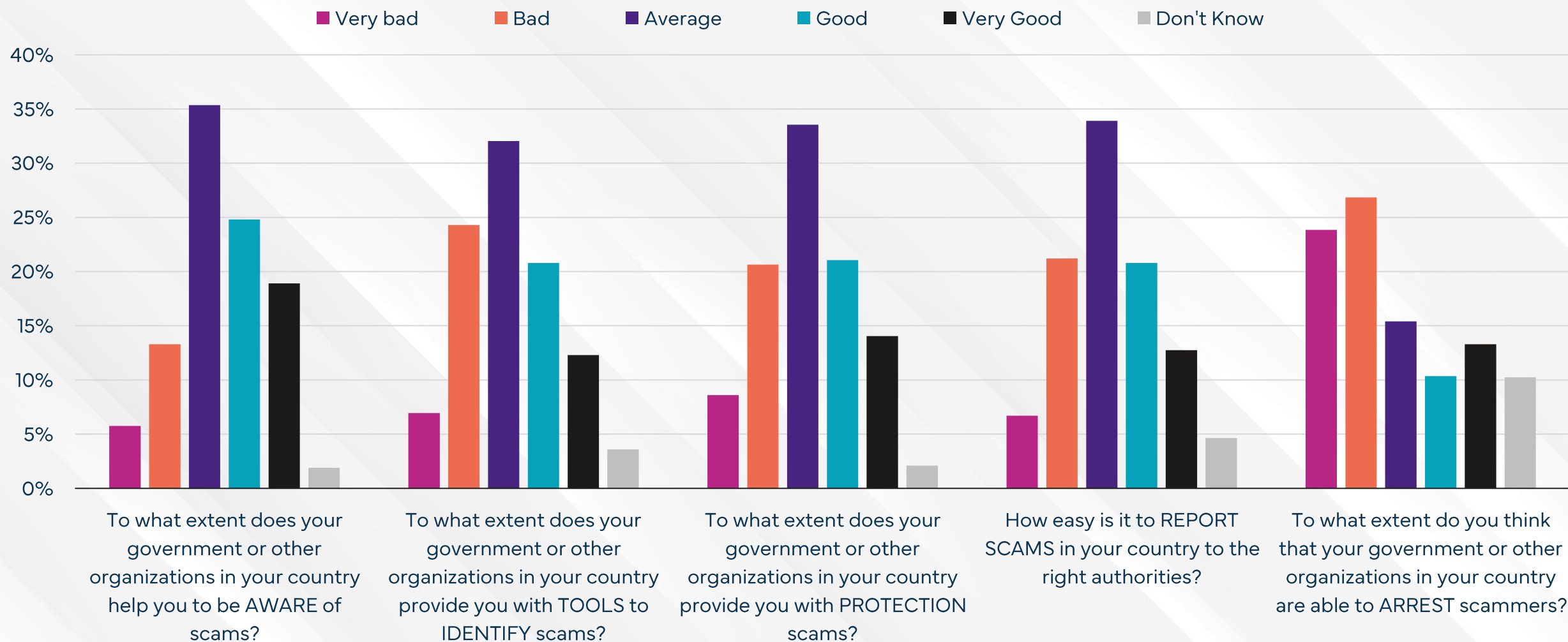Q22 – What reasons might you have to not report a scam?

# 11% of Britons assume no one will refund their scam losses



Respondents (%)

| Category | |
|---|---|
| Government | |
| Police | |
| Consumer Agency/General Complaints Board | |
| Financial Supervisory Authority | |
| Online platform used by the fraudster | |
| The website provider/host used by the fraudster | |
| My bank, payment method or crypto exchange I used | |
| My telecom or mobile operator | |
| Insurance company | |
| No one would refund me | |
| Other | |

**Others believe their bank, payment method, crypto exchange or online platform used will refund them.**

Q23 – If you were scammed, who do you think should be responsible for making sure you are paid back for your loss?
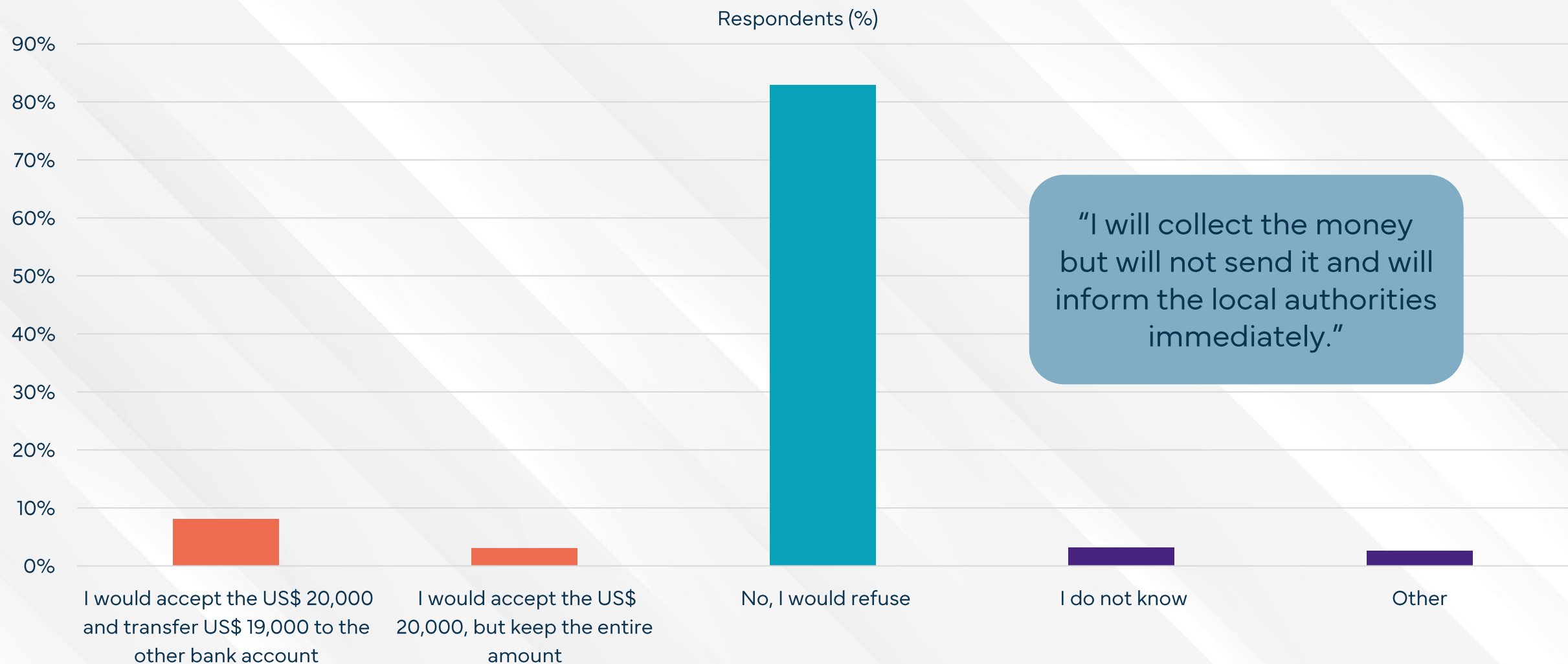
# Citizens are unhappy with the UK's attempts to arrest scammers



Legend: Very bad | Bad | Average | Good | Very Good | Don't Know

Categories:
- To what extent does your government or other organizations in your country help you to be AWARE of scams?
- To what extent does your government or other organizations in your country provide you with TOOLS to IDENTIFY scams?
- To what extent does your government or other organizations in your country provide you with PROTECTION scams?
- How easy is it to REPORT SCAMS in your country to the right authorities?
- To what extent do you think that your government or other organizations in your country are able to ARREST scammers?

Overall, 32% of the participants rate the actions of the government as (very) bad, 34% as (very) good.

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

# 11% of Britons admit that they would consider being a money mule

Respondents (%)



"I will collect the money but will not send it and will inform the local authorities immediately."

Chart categories (x-axis):
- I would accept the US$ 20,000 and transfer US$ 19,000 to the other bank account
- I would accept the US$ 20,000, but keep the entire amount
- No, I would refuse
- I do not know
- Other

y-axis: 0% – 90%

However, 83% of those surveyed would refuse to be involved in a "money mule" scam.

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

About
This Report

# Who are we?

The **Global Anti-Scam Alliance (GASA)** is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organizations to share insights and knowledge surrounding scams. GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various countries.

**Cifas** is the largest not-for-profit fraud prevention service in the UK. It has more than 750 members who represent various industries including banking, retail, insurance, and telecoms. Cifas protects businesses and individuals from fraud through effective and secure data and intelligence sharing between the private, public and third sectors. Additionally, the independent organisation offers a range of products and services to help businesses prevent fraud and delivers specialist training for counter-fraud professionals through its Cifas Fraud and Cyber Academy.

Cifas' data is included in the Office of National Statistics England and Wales Crime Statistics of police recorded crime and it works alongside law enforcement agencies in tackling fraud. In 2023, Cifas members prevented more than £1.8bn of fraud losses.

1. Survey Administration:

- Tool Used: Pollfish.com

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

2. Incentives and Fraud Prevention:

- Incentives: Non-monetary perks, such as extra lives in games or access to premium content.

- Fraud Prevention: Advanced AI and machine learning technologies to remove biased responses and enhance data quality.

3. Data Correction and Estimation Challenges:

- Statistical Corrections: Adjustments made based on the general demographic distribution within each country to account for potential biases in age or education level.

- Estimation Limitations: Outliers were removed as needed, and losses under one bitcoin were not included due to reporting constraints.

4. Additional Data Sources:

- Inhabitants per country: Worldometers.info

- Currency conversion: Xe.com

- Internet penetration: Wikipedia

- GDP Estimate 2024: Wikipedia

5. Translation and Localization:

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

6. Inspirational Reference:

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

# About the authors

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

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

**Clement Njoki** is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.

**Sam Rogers** is GASA's Director of Marketing. Previously, he worked in Risk Advisory, before transitioning into a career as a researcher, copywriter, and content manager specialized in cutting-edge electrical engineering topics, such as photonics and the industrial applications of electromagnetic radiation.

Sam left the world of corporate industry seeking a role which would allow him to concentrate on networking and events management, while allowing him to contribute something worthwhile to society.

**James Greening**, operating under a pseudonym, brings a wealth of experience to his role as a scam investigator, content writer, and social media manager. Formerly the sole driving force behind Fake Website Buster, James leverages his expertise to raise awareness about online scams. He currently serves as a Content Writer and Social Media Manager for the Global Anti-Scam Alliance (GASA) and regularly contributes to ScamAdviser.com.

# Join the Network to Defeat a Network

CIFAS — Fighting Economic Crime Together

GASA — Global Anti-Scam Alliance

## INTELLIGENCE SHARING
Regular Virtual Meet-ups
8 Topic-based Email Groups
10,000 Professionals Newsletter

## RESEARCH
Global State of Scams
30+ Regional Reports
Policy Papers

## NETWORKING
3 International Summits
Online Member Directory
National GASA Chapters

## CYBERCRIME EXCHANGE
80+ Pooled Data Sources
Realtime Data Sharing
Access to Global Leaderboards

## OUR FOUNDATION PARTNERS

amazon    Bitdefender    Capital One

feedzai    Gogolook    Google

mastercard    SCAMADVISER    Meta

TREND MICRO    Match Group

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