



The State of Scams in the United Kingdom 2023

10% of Britons fell victim to scams or identity theft in the last 12 months

The echoes of history reverberate through Britain's cobbled streets, but today, a more silent and insidious foe weaves its tale. Among the population, a diverse group of 2,000 UK citizens, slightly favouring women, most aged between 35 and 44 with vocational qualifications, stand as representatives of Britain's modern digital frontlines.

There's a hearty British confidence present. An impressive 68.6% of these respondents believe they can deftly dodge the pitfalls of scams, identifying their deceitful approaches before they wreak havoc. However, reality paints a more sombre picture. A disconcerting 62% have walked unsuspectingly into the jaws of scams within the last month alone. And it doesn't end there. Over half, 53% to be precise, attest to the burgeoning menace of such scams over the past year.

As one delves deeper, patterns emerge. The channels through which these deceptions sneak into everyday lives are primarily digital. Emails, the letters of today, top the list, accounted for by 74% of respondents. Platforms, so integral to professional and personal correspondence, like Gmail (34%) and Outlook (30%), find themselves unwilling participants in this deceit. Following closely behind is the traditional phone channel, accounting for 56% of scams. Even as phone rings and SMS chimes, familiar sounds in the cacophony of daily life, stand compromised. Instant messaging platforms aren't faring much better. With Facebook at 28% and WhatsApp at 22%, scammers find myriad ways to infiltrate the average Briton's digital sanctuary.

The scams themselves, while diverse, bear marks of familiarity. There are those phishing emails, artfully crafted to trick the unsuspecting into revealing personal information. Then, the tale as old as the internet itself, the much-cited 'Nigerian Prince' ploys. Shopping scams, a reflection of our growing digital consumerism, lead the way with 15% of respondents experiencing them. Identity theft, with its deep-reaching consequences, is a close second at 13%. The harrowing realization is that for each individual ensnared, they fall prey to an average of 1.6 scams.

The aftermath of these encounters is chilling. Online shopping scams, with their promises of irresistible deals and once-in-a-lifetime offers, have caused considerable distress for 26% of respondents. Identity theft, in all its invasive glory, has profoundly affected 24%. The theft isn't always about money. It's personal, emotional. It shakes the very foundations of trust.

While monetary losses are palpable, the psychological toll is immeasurable. Of those caught in the deceptive web, 46% have felt its lingering emotional impact. The innocence of believing in offers that sound 'too good to be true' emerges as a consistent pitfall. On reflection, many victims acknowledged their oversight of classic red flags — such as glaring spelling mistakes or the absence of security assurances on dubious websites.

But what do the Brits do when faced with such adversity? Surprisingly, or perhaps, characteristically, a vast 66% don their stiff upper lip, choosing not to broadcast their unfortunate encounters. However, a sizable 31% seek redress, primarily turning to the trusted realms of their banks or the ever-reliable local police departments. The path to recovery, particularly financial, is often thorny. While 33% manage to reclaim their lost funds, a worrying 35% see their efforts go in vain.

The sentiment resonating through this digital battlefield is clear. There's an urgent cry for heightened protection and education. Scams have ceased to be outliers. As one respondent candidly stated, "They feel like a natural part of life now." This sentiment was echoed by another: "I get so fed up with scammers it makes it hard to know who to trust."

In this modern chronicle of Britain, the challenges are clear. The nation stands at the crossroads of the digital age, grappling with deception and seeking the promise of a safer tomorrow. Armed with knowledge and a desire for change, Britain continues its march forward, ever vigilant, ever hopeful.

Cifas praises new initiatives in Britain's battle against post-pandemic scam surge

In a world rife with misinformation and scams, the United Kingdom is experiencing a substantial rise in fraudulent activities. To gain insight into the present scenario, we bring you an interview with **Mike Haley, CEO of Cifas**, a not-for-profit fraud prevention membership organization in the UK. In this dialogue, Mr. Haley shares crucial data on the burgeoning issue and illuminates the measures being taken to shield consumers.

Scams have always been a challenge for any country, but how significant is this issue in the UK today? The extent of scams in the UK is both alarming and distressing. They've long posed a significant problem, causing grave harm to each victim, a situation exacerbated by the current cost-of-living crisis and economic instability. Criminals have swiftly adapted their scams to exploit these changes, frequently targeting individuals facing financial difficulties. According to the Crime Survey of England and Wales for the year ending March 2023, the UK saw 3.7 million fraud incidents in 2022, a figure that unfortunately only represents the tip of the iceberg, as an estimated 86% of fraud cases go unreported. Specifically, reports of advance fee fraud surged year-on-year, rising from 60,000 to 391,000 offences in 2023.

Which scams were trending in the United Kingdom last year? Last year in the UK, scammers capitalized on the increased living costs, enticing victims with financial aid or investment opportunities through phishing and smishing campaigns, sometimes using fake celebrity endorsements. Impersonation scams skyrocketed, with fraudsters masquerading as banks or government agencies, leading to around £178 million in losses in 2022, as reported by UK Finance. The rise in mortgage interest rates spurred a surge in fraudulent rental ads on social platforms, resulting in a nearly 25% increase in rental fraud cases compared to the previous year. Additionally, the online shopping boom post-COVID and the demand for second-hand goods fueled a significant rise in online shopping scams and authorised push payment (APP) fraud, with losses amounting to about £485 million in 2022. Employment scams also saw a surge, with approximately 1 in 5 individuals falling prey to fake job ads seeking to harvest personal information or recruit money mules.

Which actions have been taken by your government and other organizations to protect consumers from scams? To protect consumers from scams, Cifas has been vigorously campaigning for stricter regulation of online platforms, given the considerable harm inflicted through fraudulent content hosted on these platforms. In this regard, the introduction of the Online Safety Bill by the UK Government marks a significant step forward, fostering more efficient regulation of search engines & social media platforms concerning content moderation. Additionally, we wholeheartedly support initiatives like "Check a Website," a UK extension of ScamAdviser.com, developed in collaboration between GASA and Get Safe Online. This platform serves as a vital tool for UK consumers, letting them verify websites before using them, thus combating the surge in APP fraud and the increasing number of victims falling prey to fake ads & offers online.

What action is needed now to give consumers the upper hand in the fight against scams? The coordination of regulatory actions is critical. Alongside the Online Safety Bill, the UK Government is working on the Online Advertising Programme to regulate advertisements hosted on websites outside the scope of the bill, encompassing major search engines and social media platforms. These programmes must operate in unison to prevent criminals from simply migrating to lesser-regulated platforms to bypass enhanced checks and controls. By ensuring seamless coordination, we can prevent criminals from exploiting loopholes & protect consumers more effectively.

As the government and other organisations build an arsenal of tools and strategies for UK consumers to safeguard themselves against scams, like the Online Safety Bill and "Check a Website," the changing landscape of scams means a sustained, synergised approach will be Britain's strongest weapon in this ongoing battle.



Mike Haley
CEO
Cifas



2,000 British people participated in the survey

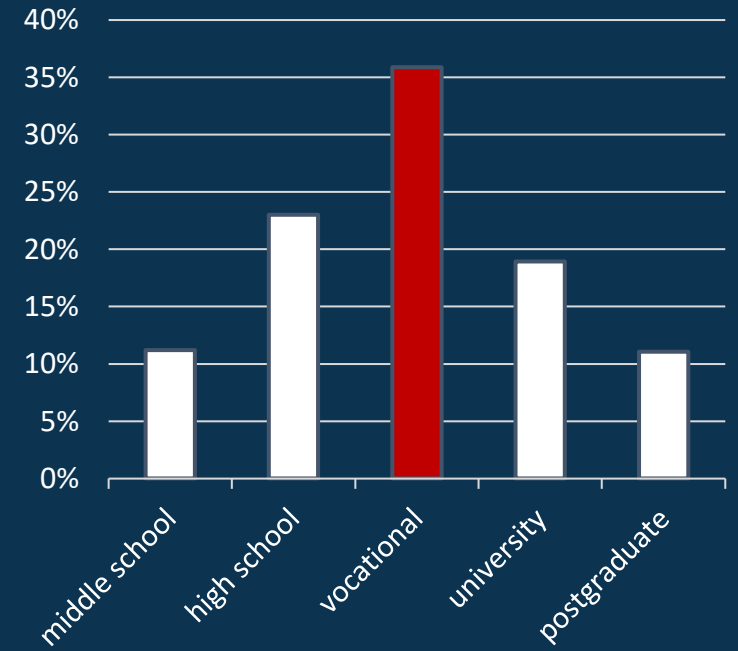
Gender



Age

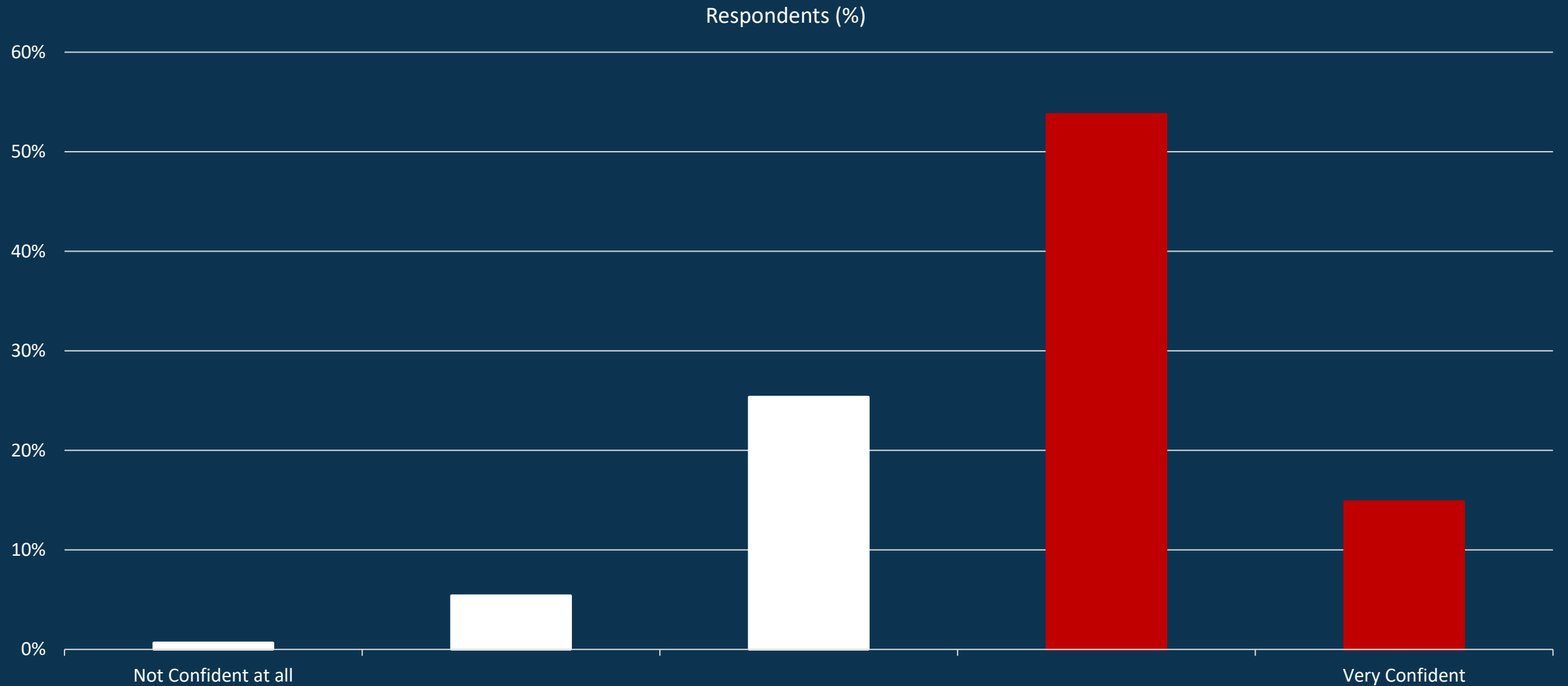


Education



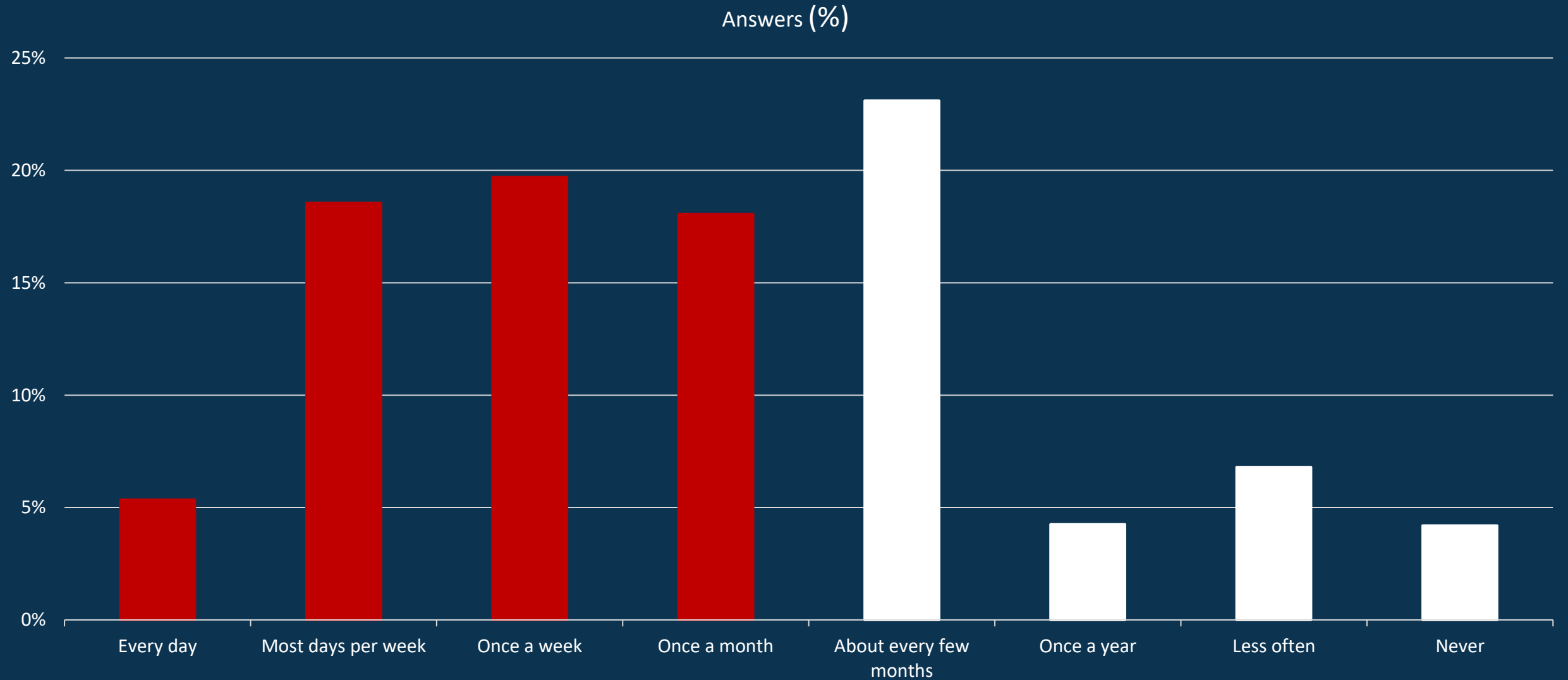
Slightly more women than men participated, mainly in the age groups 35 – 44 with a vocational education.

68.6% of Britons are (very) confident that they can recognize scams



Only 0.65% are not confident at all.

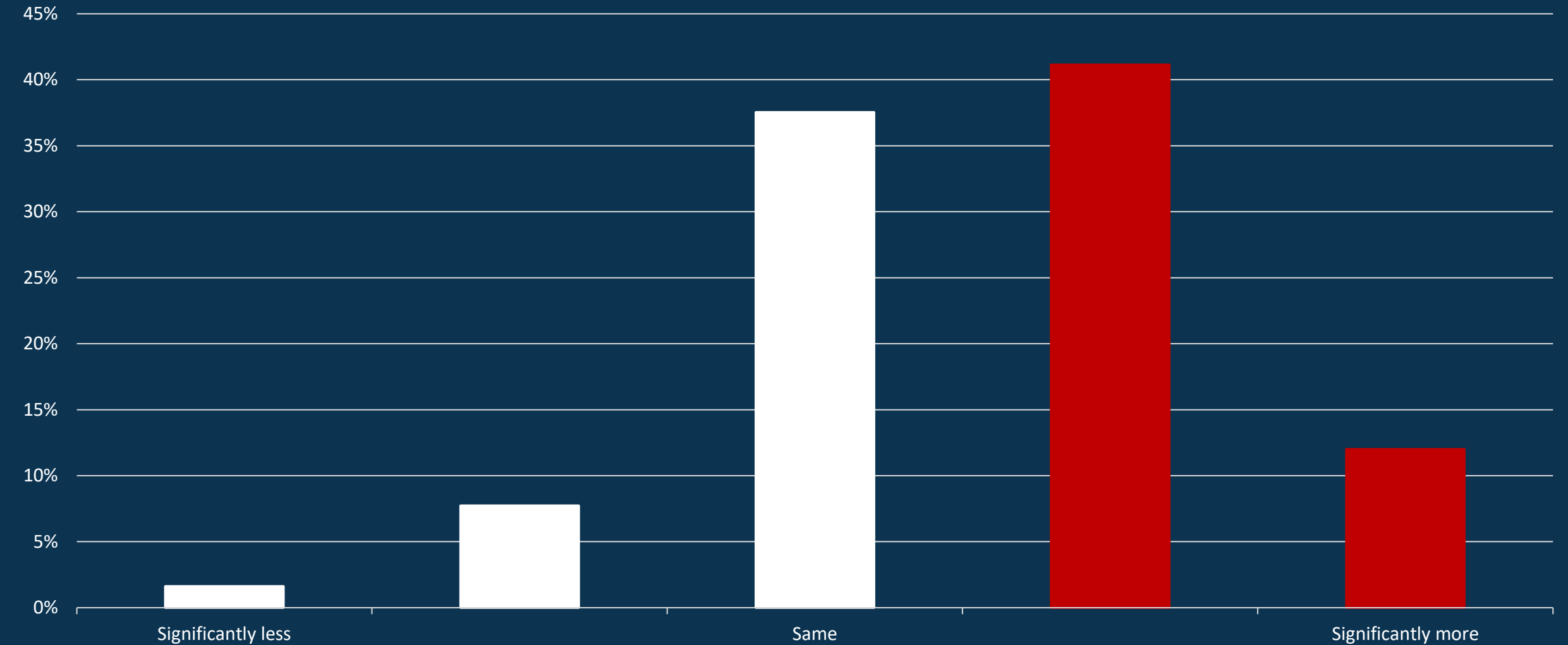
62% of Britons encounter a scam at least once per month



23% experienced a scam (attempt) at least every few months.

53% of British people experienced more scams in the last 12 months

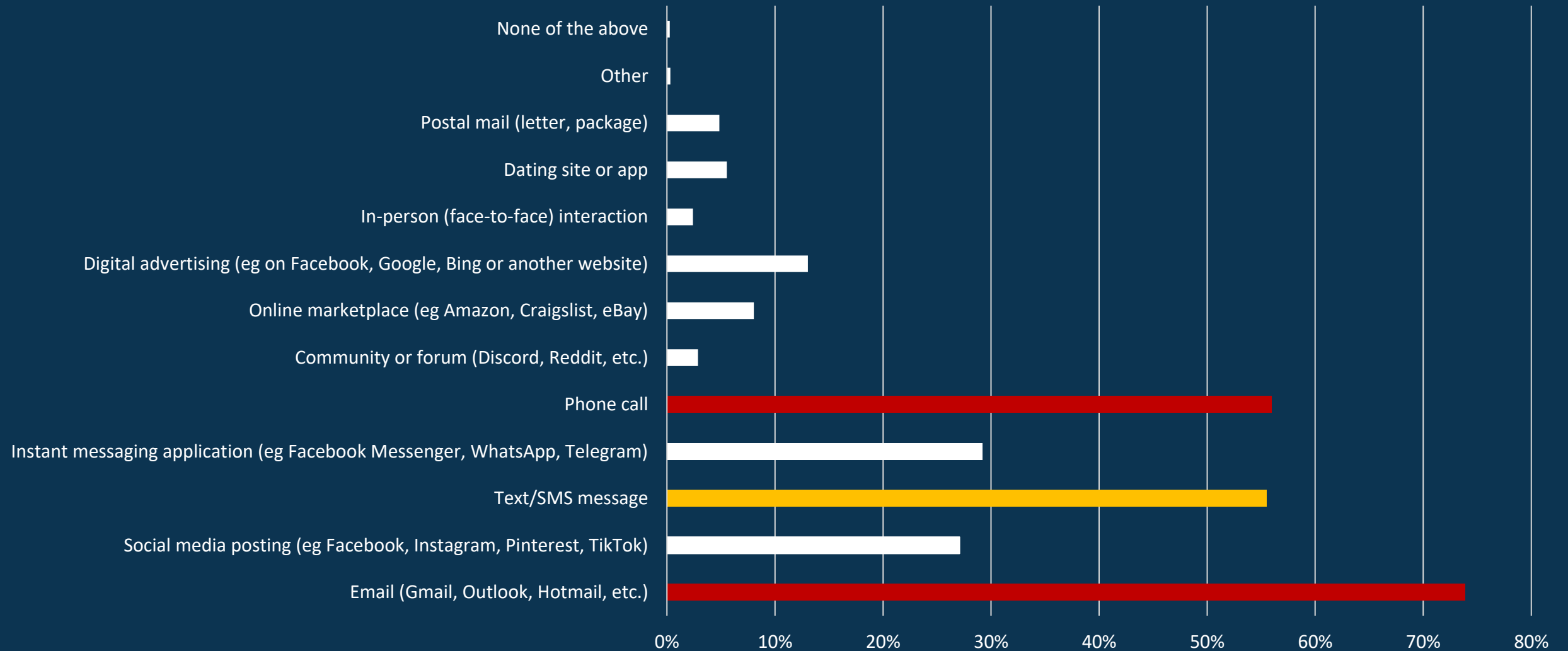
Answers (%)



Only 9% experienced fewer scams.

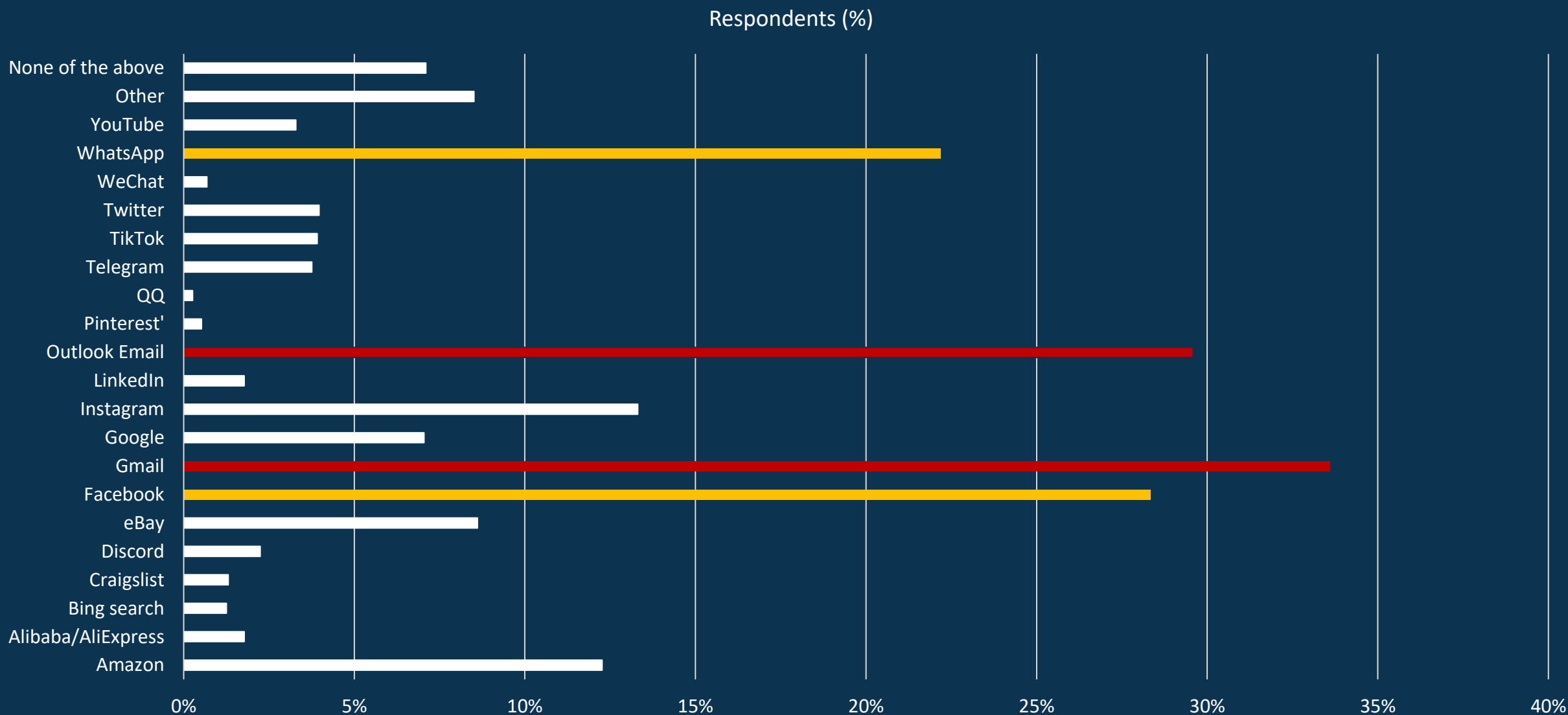
Most British people receive scams via Email and Phone

Respondents (%)



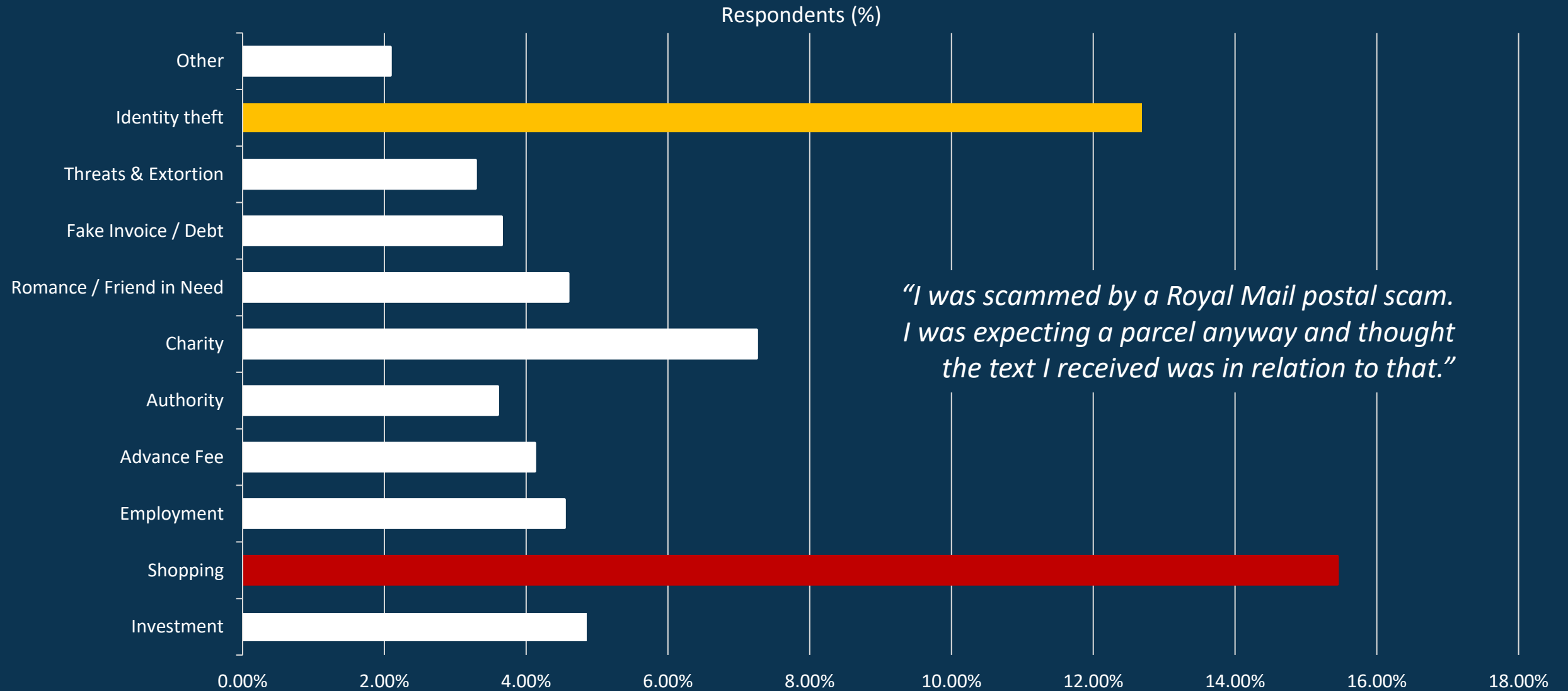
SMS messages are also common scam media.

Gmail & Outlook are the most used platforms by scammers against Britons



Followed by Facebook & WhatsApp, while Yahoo! was named several times by respondents filling in the 'other' field.

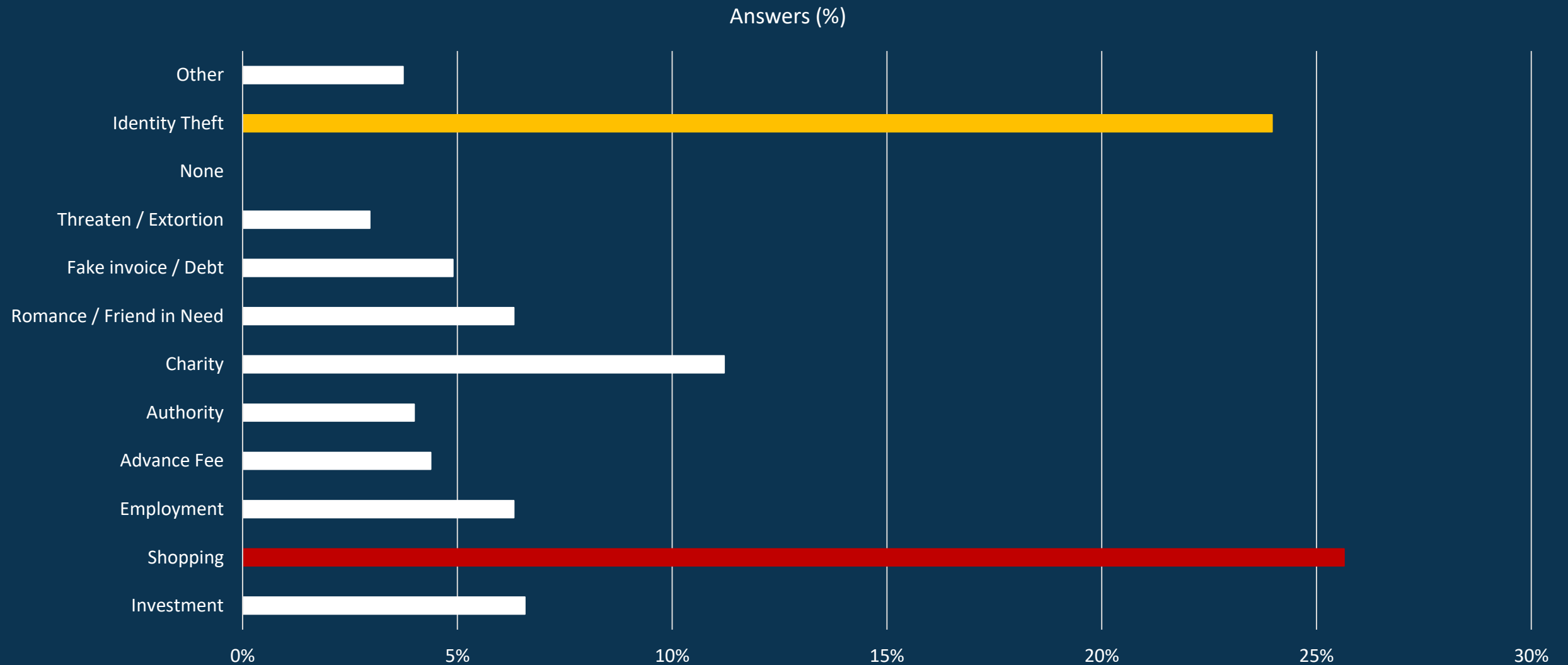
39% of the participants experience at least one scam in the last 12 months



"I was scammed by a Royal Mail postal scam. I was expecting a parcel anyway and thought the text I received was in relation to that."

Shopping and Identity Theft are the most common types of scam, while on average, 1.6 scams were experienced per scammed participant.

Online shopping scams have the most impact compared to other scams



Followed closely by Identity Theft.

Scams are hurting Britons in many ways

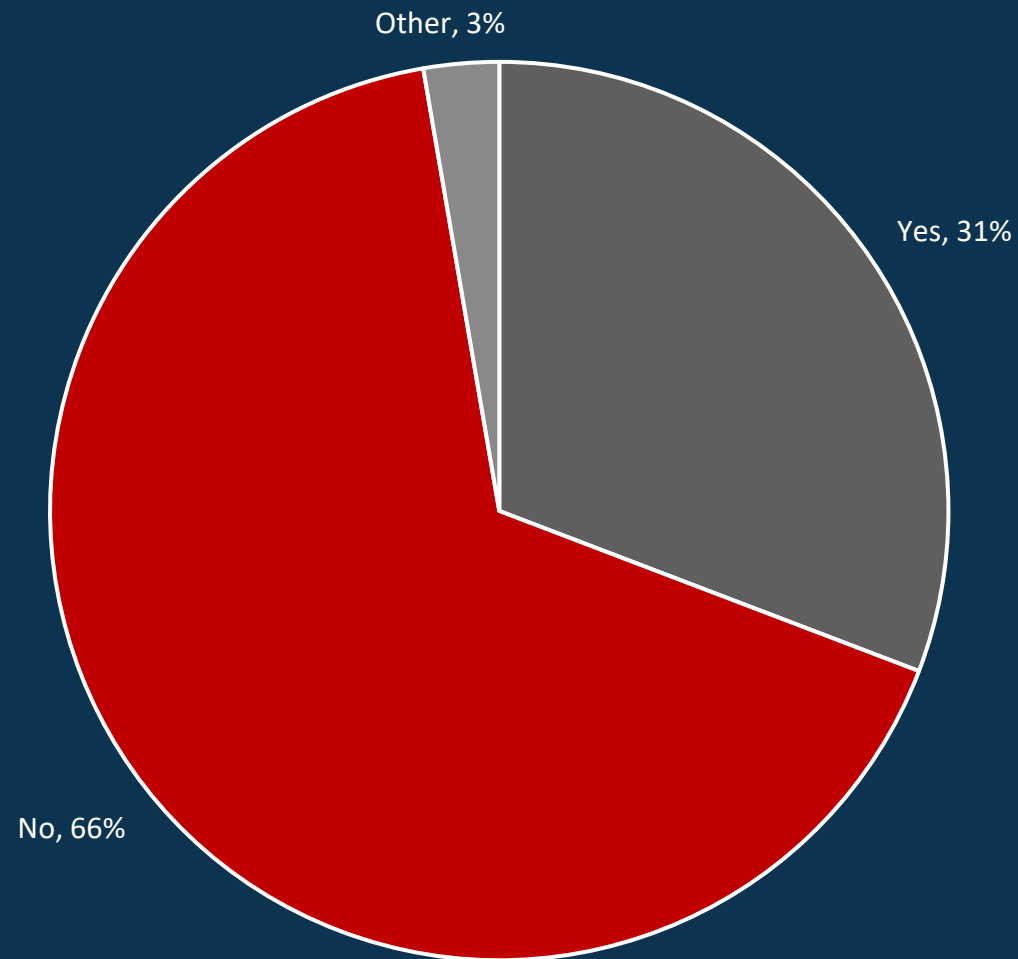
“Facebook Marketplace Fraud. The individual advertised a Nintendo Switch for sale, but upon receiving my payment, they removed the listing and blocked me without delivering the product.”

“I opened an email that appeared to be from a government source, but quickly navigated away upon realising its suspicious nature. Later, I discovered that funds had been withdrawn from my account.”

“I invested money in a website with the expectation of receiving Bitcoin and having them conduct online trading on my behalf. Unfortunately, the promised transactions never materialized, and I was left without my initial investment being returned to me.”

“Someone sent me an email saying they could see my search history and threatened to harm me and send it to my friends and family if I didn’t send them money.”

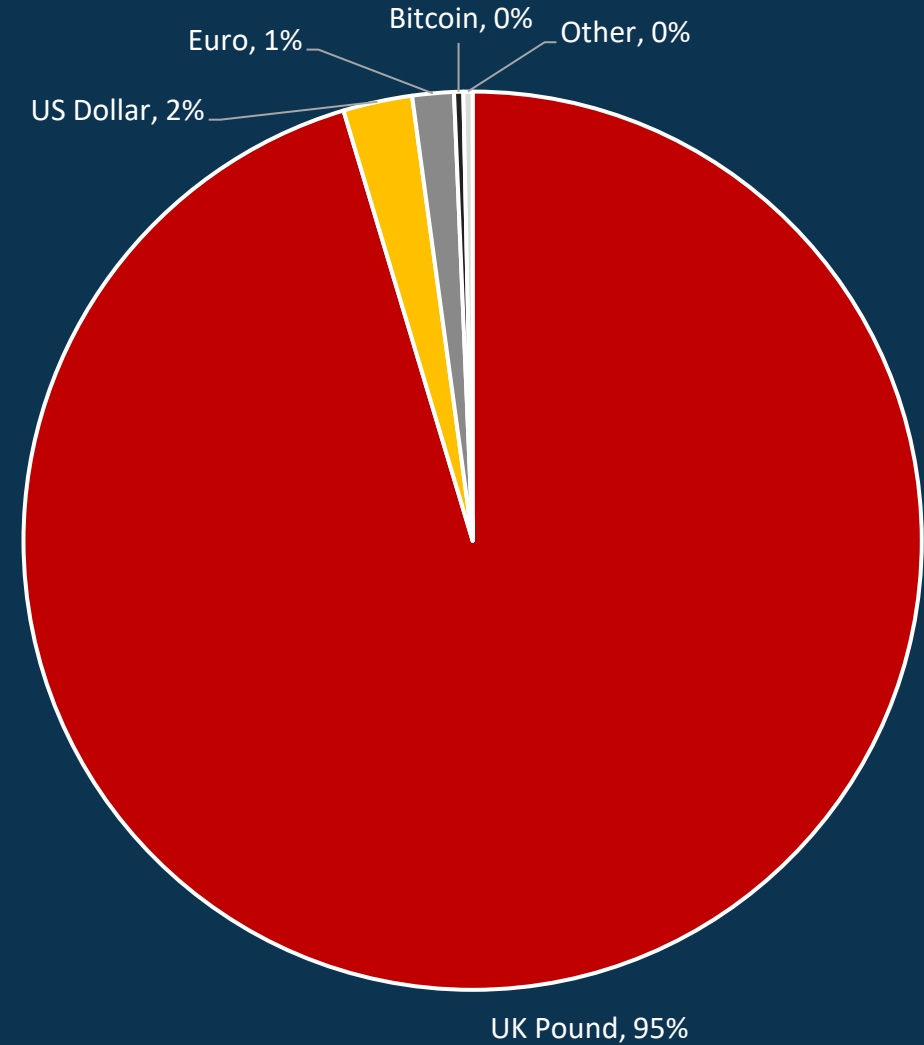
66% did not report the scam to law enforcement



31% stated having reported the scam to law enforcement or another government authority.

10% of Britons reported having lost money in a scam last year

Survey Key Statistics	
Number of persons approached	6,325
Participants completing the survey	2,000
Participants losing money	603
% losing money / approached persons	10%
Average amount lost in US Dollars	\$ 1,817
Total country population	67,763,530
Population over 18 years	53,688,185
# of people scammed > 18 years	5,118,415
Total amount lost in scams*	\$ 9,300,160,250
Gross Domestic Product (\$ millions)	3,158,938
% of GDP lost in scams	0.3%

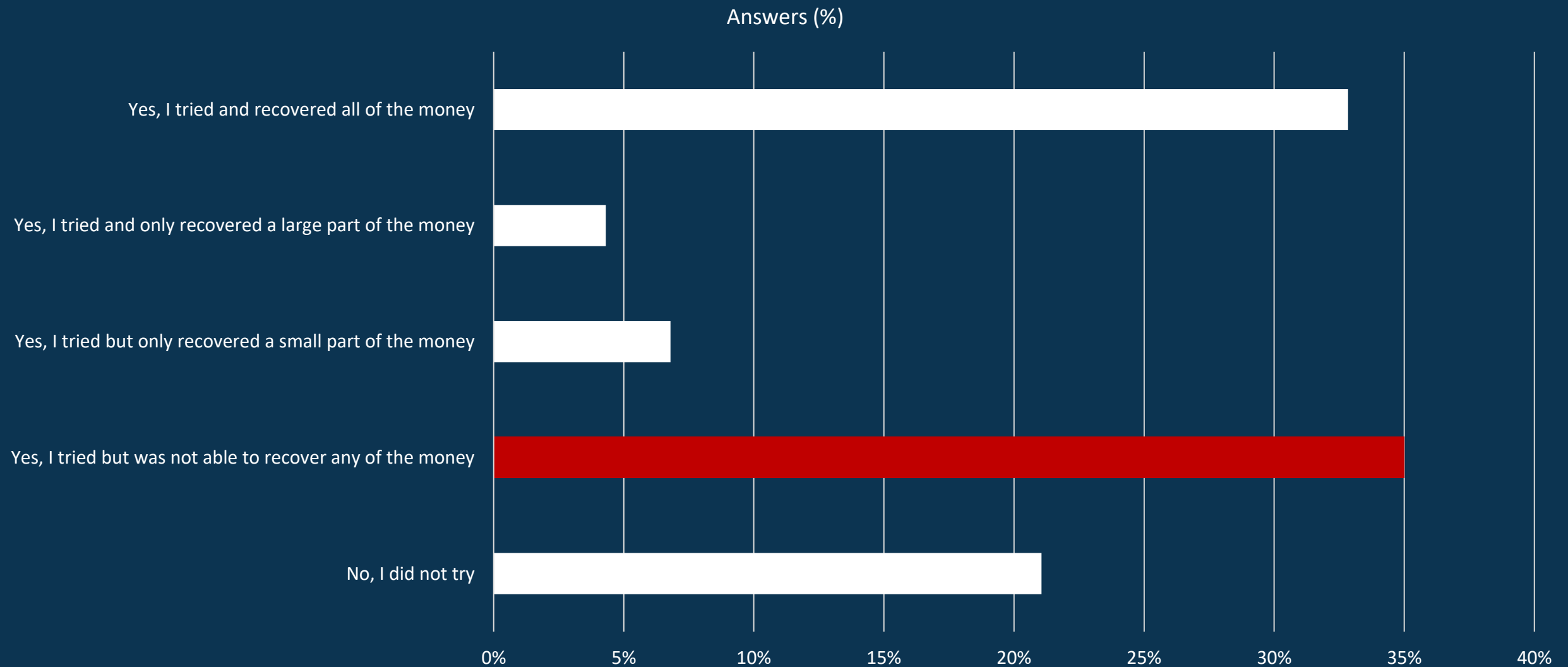


Nearly all scams were reported in Pounds (95%) with a few cases in US Dollars (2%), Euro (1%) and some Bitcoin (2).

* Bitcoins were excluded from the total amount lost due to an error in the survey questionnaire. 2 extreme amounts were also omitted from the results.

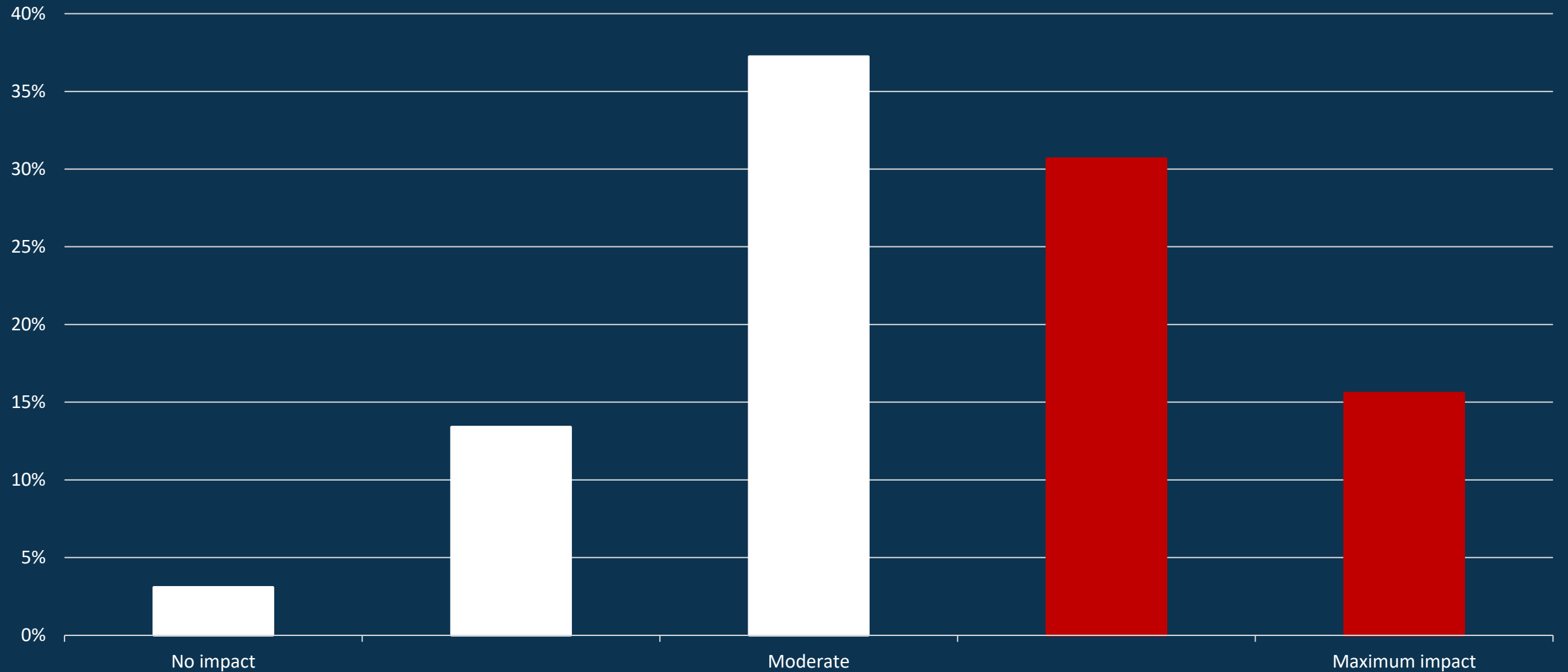
Q11 / 12: Think about the incident that has had the most impact. In total, how much money did you lose before trying to recover the funds? Only enter a round number. If no money was lost enter "0".

33% of the participants in the survey were able to recover all money lost



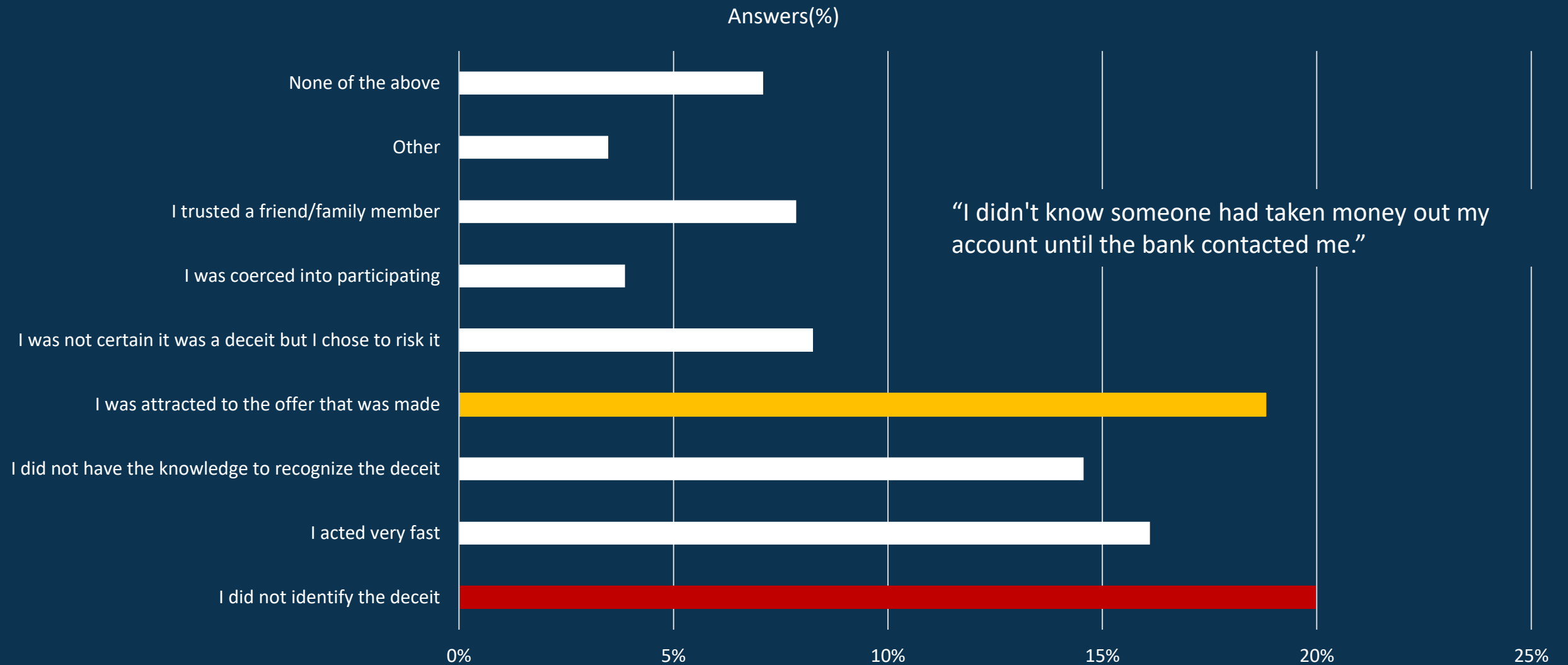
21% did not try to recover their funds. 35% tried but was not able to recover any money.

46% of the scam victims perceived a (very) strong emotional impact



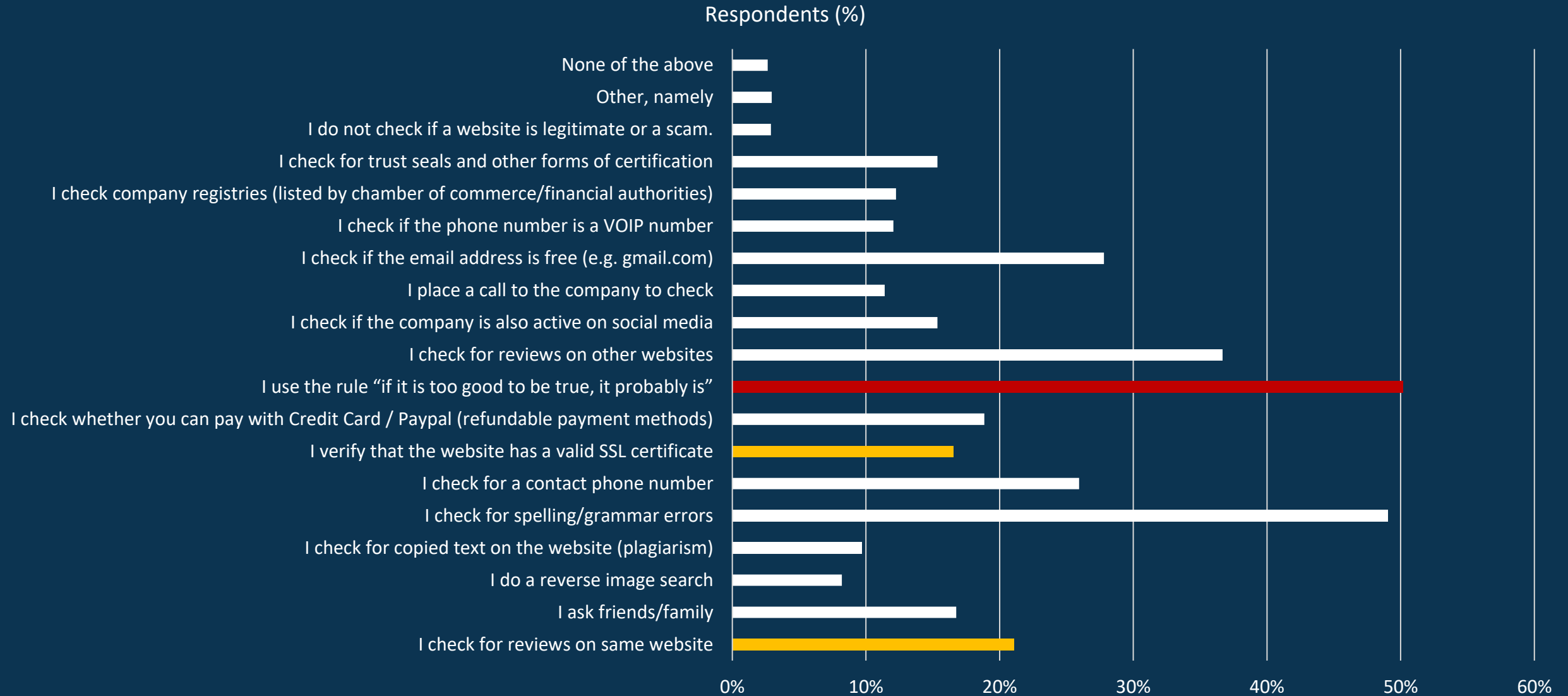
Only 16% of the participants reported no or minor emotional impact.

The main reasons the British fall for scams is they do not identify the scam



Several victims also reported they were attracted to the offer being made.

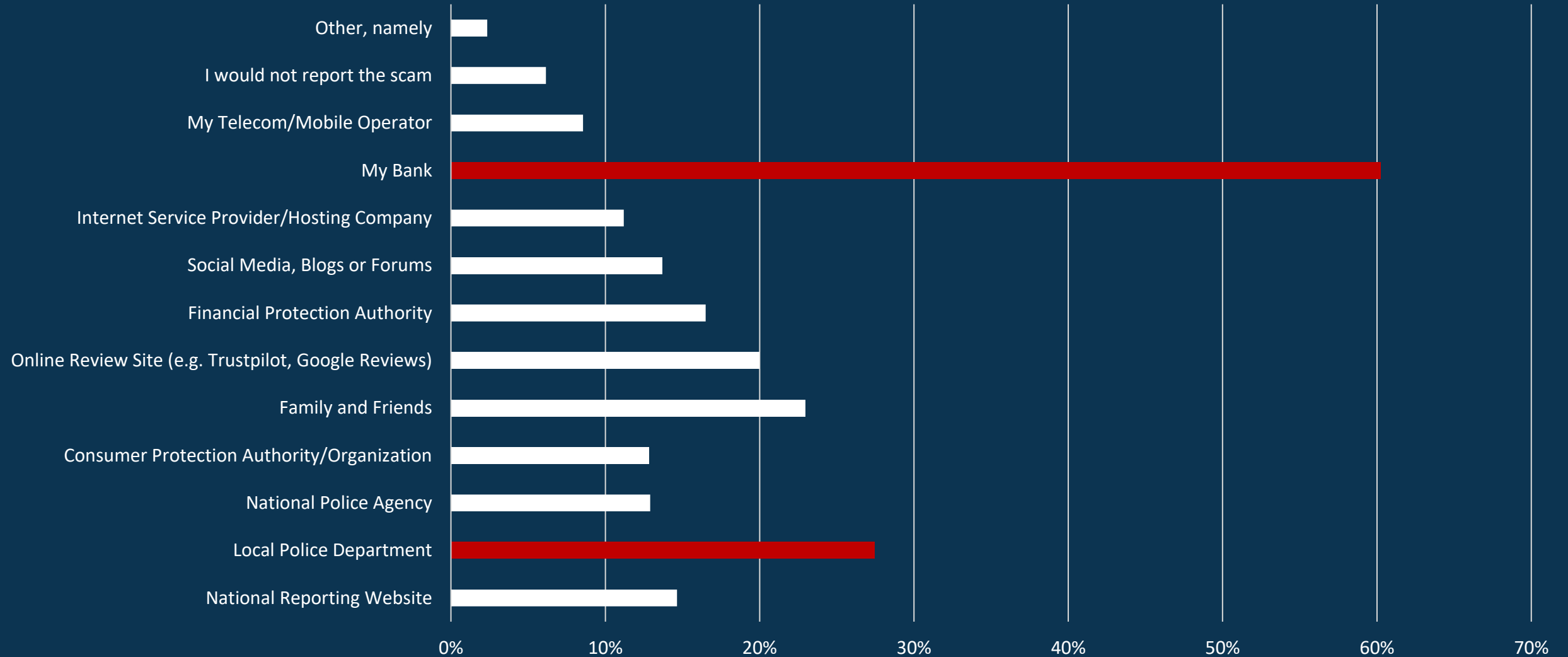
The most common way to check for scams is the rule “if it is too good to be true”



Several “unsafe” methods like checking the SSL certificate and reviews on the same site are often used as well.

Scams are mostly reported to Banks and Local Police Department

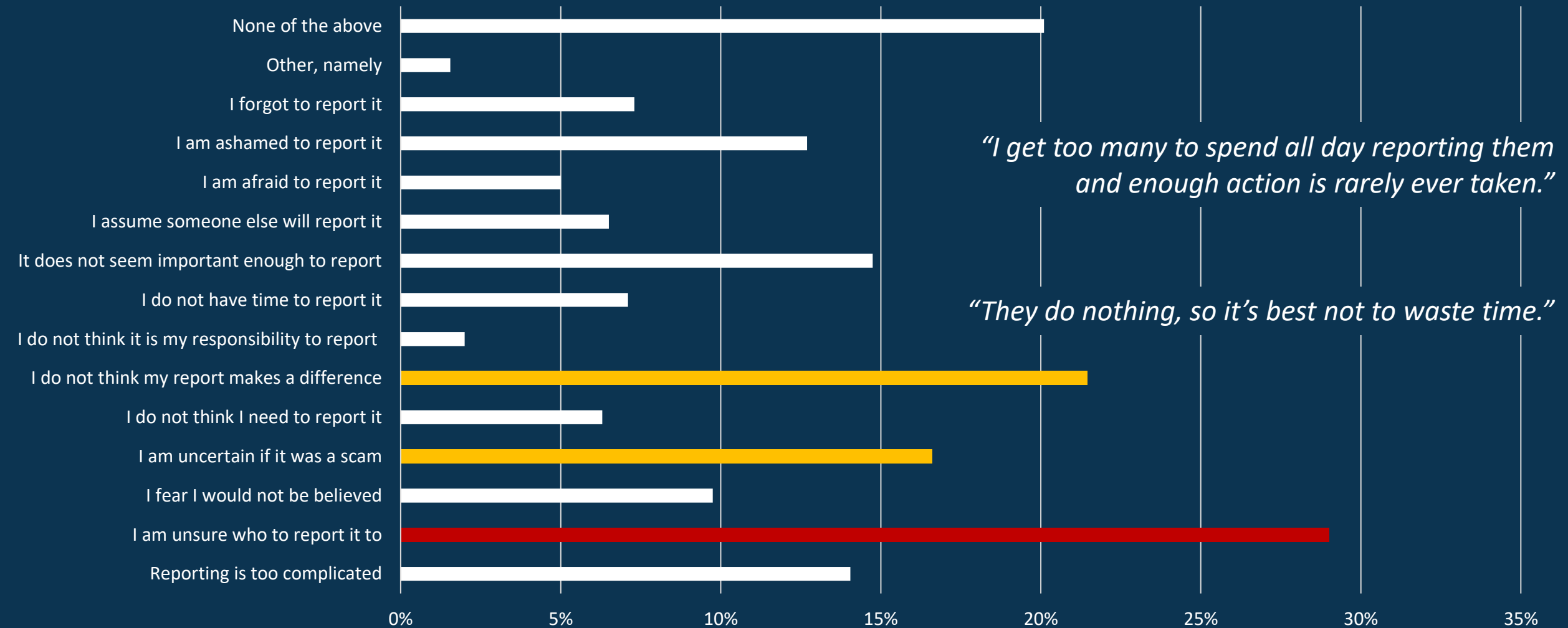
Respondents (%)



Family and Friends, Online Review Sites and Financial Protection Authority are also popular recipients of scam reports.

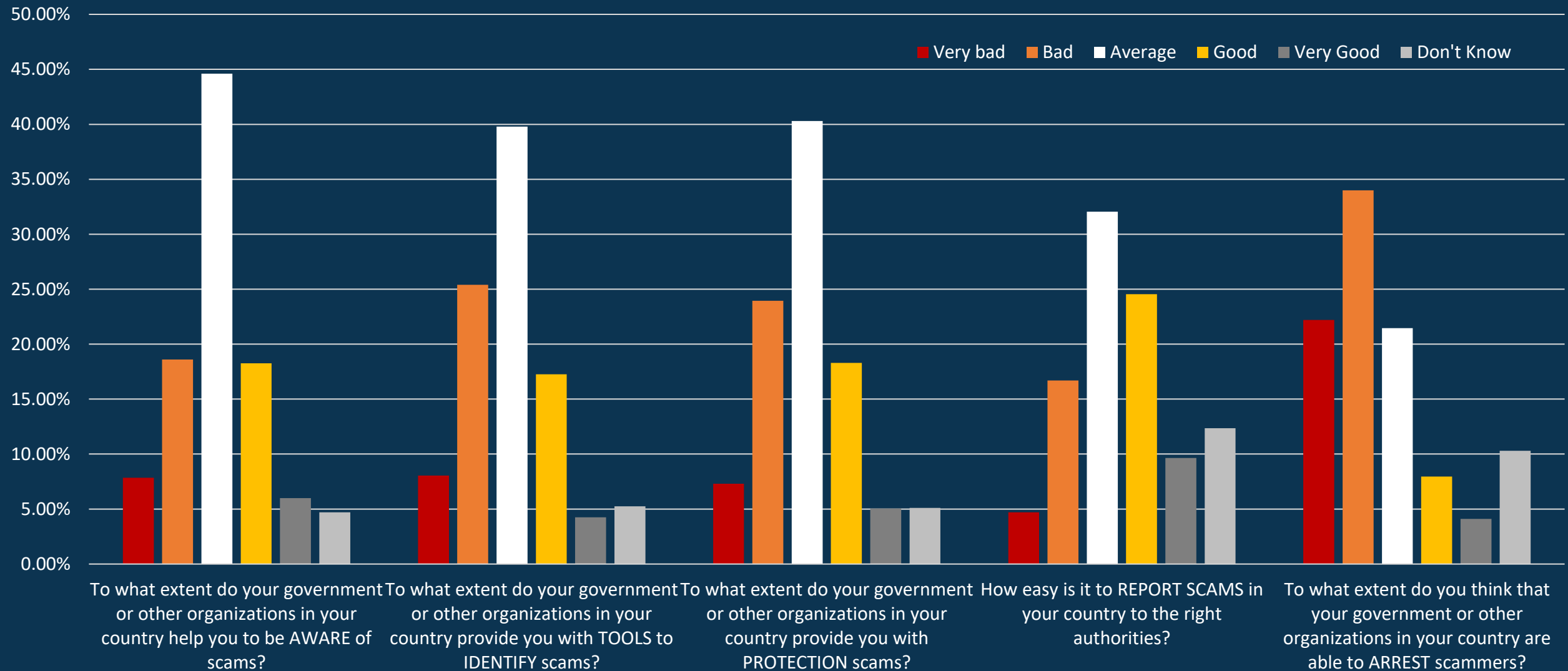
Key reason for not reporting a scam is the uncertainty of where to report it

Respondents (%)



Additional significant factors for refraining from reporting include the belief that it won't yield any impact and the hesitancy stemming from uncertainty about whether it was a fraudulent scheme.

The British are not pleased about the number of arrests & identification tools



Overall, 34% of the participants rate the actions of governments as (very) bad, 14% as (very) good.

Some remarkable quotes

“When I’ve reported on the past, nothing has been done about it so it’s seems a waste of time“

“I have only known relatives to be scammed and once nearly twice but she caught on. Unfortunately, its very hard to know who to report it to.”

“They feel like a natural part of life now so I think people don’t think their reports would do anything.

“Governments and companies hosting the scammers should be doing more efforts to trace, block and prosecute.”

“I get so fed up with scammers it makes it hard to know who to trust.”

About this Report



Who are we?



GASA's driving mission is to shield consumers globally from the financial and emotional trauma of scams. With many cybercriminals operating freely in the digital space, GASA invites governments, law enforcement, consumer protection, financial authorities & providers, brand protection agencies, social media, ISPs, and cybersecurity companies to share knowledge and define joint actions. These connections culminate in the annual Global State of Scams report, which follows the release of detailed reports that delve into the scam impact on individual countries each year.

For more information, or to arrange an interview with GASA Managing Director, Prof. Jorij Abraham, please contact Sam Rogers, GASA Marketing Director at +31 (0) 645 130 670 or sam.rogers@gasa.org.

Cifas is an independent, not-for-profit membership organisation that protects businesses and individuals through effective and secure data and intelligence sharing between the private, public and third sectors. In 2023, Cifas member organisations prevented around £1.3 billion of fraud losses.

Cifas data is included in the Office of National Statistics England and Wales Crime Statistics of police recorded crime and works alongside law enforcement agencies in tackling fraud.

For more information, or to arrange an interview with Cifas CEO, Mike Haley, please contact Hayley Paterson, Cifas Press and PR Manager, on +44 (0) 20 4551 7072 or press@cifas.org.uk.



Special Thanks & Methodology

Special Thanks

We would like to thank Professor Mark Button, Co-Director of Centre for Cybercrime and Economic Crime at the University of Portsmouth, and Jack Whittaker, PhD Candidate Criminology at the University of Surrey, for their feedback and support.

Methodology

We used Pollfish.com to set-up the consumer survey and get participants. Pollfish utilises a survey methodology called Random Device Engagement. RDE is the natural successor to Random Digit Dialing (RDD). Our survey was delivered via Pollfish inside popular mobile apps, RDE utilizes the same neutral environment as RDD, and an audience who are not taking premeditated surveys, by reaching them inside mobile apps they were using anyway.

Pollfish uses non-monetary incentives like an extra life in a game or access to premium content. With additional layers of survey fraud prevention including AI and machine learning, Pollfish removes potentially biased responses, improving data quality even further.

In addition to Pollfish we used the following sources:

- Inhabitants per country: [Worldometers.info](https://worldometers.info)
- Currency conversion: [Xe.com](https://xe.com)
- The country flag on the cover: wikimedia.org
- Internet penetration: [Wikipedia](https://wikipedia.org)
- GDP Estimate 2023: [Wikipedia](https://wikipedia.org)

The survey itself has been partly inspired by DeLiema, M., Mottola, G. R., & Deevy, M. (2017). Findings from a pilot study to measure financial fraud in the United States. Available at SSRN 2914560.

Feedback is greatly appreciated. You can contact us at partner@gasa.org

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 and European Ecommerce Association) and the Ecommerce Foundation.

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



Marianne Junger is Professor Emeritus of Cyber Security and Business Continuity at the University of Twente. Her research investigates the role of human factors of fraud and of cybercrime, more specifically she investigates victimization, disclosure and privacy issues. The aim of her research is to develop interventions that will help to protect users against social engineering and to increase compliance.

She founded the Crime Science journal together with Pieter Hartel and was an associate-editor for 6 years.



Sam Cajigal, as Partner Manager at GASA, leverages his background in customer relations, sales, dispute resolution, and claims management not only to expand the reach across diverse demographics but also to combat deceptive practices and fraud, thereby enhancing the mission of GASA to protect individuals from scams and fraudulent activities.



Luka Koning is a Researcher/PhD Candidate at the University of Twente. His research focuses on victimization of fraud and cybercrime, in particular the prevalence, risk factors, impact, and willingness to report. His work includes victim studies and experiments, aimed at how victimization arises and subsequently how it could be prevented.



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 Director of Marketing at GASA. Before moving into marketing management, he worked as a copywriter and content manager, specializing in cutting-edge areas of electrical engineering, such as photonics and the industrial applications of electromagnetic radiation. Sam left the world of industry in search of fulfilment and now uses his skills to expose the impact of online scams to a global audience.

Interested in participating in this report next year? Please contact jorij.abraham@gasa.org.

The Global Anti-Scam Alliance is supported by the following organizations

Foundation Partners



Corporate Partners



If you like to become a Partner, please contact Partner@GASA.org

Disclaimer

This report is a publication by the **Global Anti-Scam Alliance (GASA)** supported by **Cifas**. 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 not allowed 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

Email: partner@gasa.org

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

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

