TRENDS BioCatch

The State of Scams in the United Arab Emirates - 2024

GASA
Global Anti-Scam Alliance

Scams have become a significant issue in the UAE

How big have scams become in UAE?

Scams have become a significant issue in the UAE, with tens of thousands of residents losing life savings to fraudulent schemes. A recent study reveals that 90% of UAE consumers are at risk of responding to scammers, as 9 in 10 people are likely to overlook common fraud warning signs. Even more alarming is that 17% of the victims have been tricked multiple times, against the global average of 15%. Last year, over 40,000 UAE residents have lost millions to Ponzi and pyramid scams, crypto fraud, and bogus trading platforms. While people are generally wary of password reset requests, scammers employ extremely persuasive tactics, such as claiming a parcel is held up at customs, notifying about a subscription expiration, or offering a free voucher for a popular brand. About 77% of people in the UAE would happily press forward if a message had a positive hook, like “free gift”, “you’ve been selected”, or “you’re a winner”. Common scams include falsely advertised products on online platforms and fraudulent websites.

Scam methods such as fraud, phishing, and spoofing are significant threats, comprising 55% of the total cyber incidents in the UAE. They often involve sophisticated social engineering tactics to deceive victims into unwittingly disclosing sensitive information or credentials. Overall, 44% of UAE retailers were affected by fraudulent incidents related to cyberattacks.

Which scams stood out in the last year and were trending in UAE?

In 2023-24, notable scams included BlueChip, which swindled Dh250 million, and the Sky Media and Metaverse Foreign Exchange (MTFE) schemes, which targeted thousands of people. SkyMedia is an “earning app” that claims partnerships with YouTube, TikTok, and Facebook, promising a daily income of Dh128 just for watching videos and interacting with posts. Likewise, MTFE promises an earnings bonanza of $40 each week with just a $500 investment into cryptocurrency. MTFE's Dubai Support Team alone boasts nearly 10,000 members on Facebook, while their Telegram channel has over 71,000 subscribers. Typical investments by users into fraudulent schemes range from $1000 to $25,000. Many UAE residents also fall victim to superfluous forex and stock trading platforms. These scams often involve promises of high returns and aggressive marketing, preying on educated residents blinded by the lure of quick profits. Scammers typically have professional-looking websites and may sound very knowledgeable about the securities they are trying to sell.

Also, cybercriminals purporting to be from an official body like Dubai Police or the Department of Criminal Investigation (CID) often feign urgency to spur people into action such as paying traffic fines or a credit card fee but other methods are not uncommon. Newcomers to the UAE in particular fall prey to these scams as they may feel compelled to comply with what they believe are legitimate institutional requests. Such communications originate mainly from countries such as Nigeria, India, Romania, and Pakistan using mobile numbers.

Which actions have been taken by the UAE government and other organizations to protect consumers from scams?

The UAE government has implemented stricter regulations, launched awareness campaigns, and worked with law enforcement agencies to tackle scams. Authorities have also collaborated with financial institutions to monitor suspicious transactions and block fraudulent accounts. Consumer protection agencies are educating the public on the dangers of online scams, while the Central Bank and telecommunications companies have issued advisories to warn residents about potential threats. The UAE’s Cyber Security Council has introduced a free online tool called “Stay Safe” in partnership with etisalat by e& and the Global Anti-Scam Alliance: staysafe.csc.gov.ae. The website allows people to check if a website is legitimate, or potentially an online phishing scam. Emirates NBD has launched a UAE-wide safe banking campaign after reports of customers being targeted by fraudsters. Emirates Post also proactively combats fraudulent online schemes. However, users are always recommended to do their own verification as a best practice.

Safe browsing practices include raising awareness through education, being cautious of promises of high returns, and verifying the legitimacy of investment opportunities. Authorities recommend only dealing with licensed and regulated entities and avoiding sharing personal or financial information with unknown sources. Relevance of user awareness and training in mitigating socially engineered threats is paramount. Consumers should also be aware of red flags like pressure tactics and unsolicited offers. They should inform Dubai Financial Services Authority (DFSA) or Abu Dhabi Securities Exchange (ADSE) for any suspicious activity.

What action would you like to see taken that could give consumers the upper hand in the fight against scams?

The coordination of regulatory actions is critical. The UAE authorities should strengthen awareness campaigns with etisalat by e& and du, financial institutions, and regulatory bodies; implement extensive, high-frequency campaigns targeting both individuals and organizations, focus on education around phishing, fraud schemes, and scam detection. To enhance monitoring and compliance, the Cyber Security Council should Introduce mandatory real-time threat intelligence sharing platforms, where financial institutions and consumers can quickly report and access scam alerts, ensuring faster response and prevention of widespread damage. The government has already introduced consumer protection laws and telemarketing regulations, but expanding these initiatives with real-time fraud reporting systems and faster resolution of disputes could further empower consumers. By enforcing stricter regulations on online investment and trading platforms to ensure they are properly licensed, the Council can give consumers a clear understanding of legitimate versus fraudulent businesses.

His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security of United Arab Emirates

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

50% of the survey state to have been approached by an AI scam

The 2024 State of Scams in United Arab Emirates report is an annual study conducted by the Global Anti-Scam Alliance (GASA), Trends Research and BioCatch.

This year's survey was completed by 1,964 UAE citizens. The demography of respondents to the State of Scams in United Arab Emirates 2024 survey consists to a large degree of participants with a university degree (59%) and postgraduates (24%).

65% of the participants are (very) confident in their recognition of scams. Only 9% of respondents do not trust in their own ability to reliably identify scams. According to the survey data 56% of the UAE population receives a scam at least once per month. Only 12% of survey respondents stated that they are rarely confronted by scams.

It seems that the number of scam approaches has stabilized. 20% stated approximately the same number of approached, while 43% encountered more scams and 37% less scams compared to last year.

Most UAE citizens are aware scammers can use AI against them. Awareness of AI generated text & images is high, with complex AI chats & videos marginally less known. 50% of the respondents believe they have encountered an AI scam in the last 12 months. 30% of respondents were uncertain, while 20% believes they were subjected to scams utilizing artificial intelligence.

The majority of scams are delivered via Instant Messaging tools. WhatsApp is by far the most misused as scam delivery platform. Phone calls and Text/SMS messages are also common scam media followed by email at the 4th place. Gmail, Facebook, Instagram and Outlook round out the top five most popular digital platforms for scammers.

Shopping Scams & Identity Theft are the most common scam followed by investment scams on the 3rd place. 1.77 scams were reported per victim, suggesting that scam victims are likely to be retargeted. Only 30% of the UAE state to have reported scams to law enforcement.

49% of scams are completed within 24 hours of first contact. 33% were scammed in a matter of minutes, but 7% were targeted with a long con of a year or more. 69% came to their own conclusion that they had been scammed. 21% were notified by banks, while friends/family also often notify victims they are being scammed.

In total, 27% of UAE survey participants reported having lost money to a scam. The average amount lost was US$ 2,194.

Credit Cards & Bank Transfer are the top scam payment methods. PayPal and peer-to-peer apps are also popular tools which scammers use to collect stolen funds.

Only 9% of victims in the survey were able to fully recover their losses. 19% did not try to recover their funds. 57% tried but were not able to recover any money. 10% of the survey respondents assume no one will refund their scam losses. Others believe their bank; the police or consumer protection agency will refund them.

59% of UAE victims perceived a strong emotional impact. As a result, 62% of the UAE have less in trust the Internet because of scams.

The reason why the scammer was able to steal money or personal information differs. 23% of the respondents were attracted by the offer of the scammer. 30% reported they did not detect the scam until it was too late or lacked the knowledge to recognize the scam.

32% of the respondents check the email address and review sites (31%) in order to determine if a website is legit or a scam. Other ways to check if a website is real or a scam are asking friends & family (26%).

Likewise, scam experiences are mostly shared Family & friends (30%). Local police (29%) and banks & payment providers (28%) are the 2nd and 3rd most common place to report scams.

18% of the respondents shared that they do not know who to report a scam. Other reasons for not reporting a scam are that the process is too complicated (15%), the participant is unsure if it was a scam (15%) and the believe that reporting a scam does not making a difference (15%).

Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

Fraud Evolution, Results, and Future Perspectives

BioCatch GASA Global Anti-Scam Alliance

Tracking the Evolution of Fraud in the UAE

The UAE's fraud landscape is increasingly complex. The State of Scam Report UAE 2024 shows phishing attacks rose by 25% as fraudsters exploit new digital channels. Fake job offers and investment scams have affected 20% of residents, while 15% reported falling victim to fraudulent e-commerce transactions.

His Excellency, Dr. Al-Kuwaiti highlights the need for a proactive and collaborative approach to combat these threats, emphasizing that a coordinated response is essential for building a resilient digital ecosystem capable of addressing fraud attempts as they arise.

Key Findings and Regional Comparisons

The report shows that 35% of UAE residents experienced scams last year, higher than most European markets. While synthetic identity fraud is emerging in Europe in specific areas, the UAE faces a distinct challenge with social engineering scams, particularly fake job offers, which exploit new digital users. On the other hand, fraudsters in Europe often leverage mule accounts for rapid transfers within the same institution and instant payments to external accounts, such as those on multiple platforms. And it is only a matter of time before these new trends become prevalent in the UAE region as well.
This underscores the importance of a proactive, intelligence-driven approach to fraud prevention. Behavioral intelligence technology enables early risk identification, allowing institutions to act before significant damage occurs—a crucial approach in a market where fraudsters are constantly adapting.

Future Perspectives on Fraud Prevention

As the UAE's digital economy expands, fraud tactics are likely to become more sophisticated. This evolution underscores the importance of proactive intelligence-driven fraud prevention strategies, where behavior-based intelligence and anomaly detection allow financial institutions to detect subtle cues and address suspicious activity early on.

The report highlights the urgent need for vigilance: 40% of respondents worry about identity theft, and nearly 60% have faced phishing attempts. Addressing these risks calls for advanced fraud prevention tools and a comprehensive approach that includes regulatory support, consumer education, and cross-sector collaboration.

Concluding Thoughts

While the UAE and Europe face similar fraud challenges, each region requires a tailored strategy. The UAE's rapid digital adoption necessitates agile detection systems capable of adapting to shifting fraud patterns. As these schemes evolve, behavior-based intelligence remains a powerful defense against fraud, helping the UAE foster a secure digital landscape. With innovative solutions, the country can build a foundation of trust and resilience within its digital ecosystem.

MARKET ANALYSIS & BIOCATCH'S ROLE IN FRAUD PREVENTION

Understanding the UAE Fraud Landscape

The UAE's swift adoption of digital technologies has accelerated progress but also driven a notable rise in digital fraud. According to the State of Scam Report UAE 2024, 35% of UAE residents encountered digital fraud last year, up by over 10% from the previous year—a trend reflecting the global connection between online services and fraud growth.

His Excellency Dr. Mohamed Al-Kuwaiti, Head of Cyber Security for the UAE, has underscored the importance of adaptive strategies, stating that security measures must evolve as rapidly as fraud tactics to ensure a safe digital environment. The UAE's collaborative approach involves government agencies, financial institutions, and technology providers working together to enhance consumer protection and regulatory frameworks.

BioCatch supports these efforts by offering behavior-based intelligence solutions tailored to the region's specific fraud challenges, such as social engineering scams, account takeovers, and phishing attacks. As fraud becomes more sophisticated, technologies like behavior analysis are essential for early detection and prevention.

Differences in Fraud Dynamics: UAE vs. Europe

The UAE and Europe face different fraud threats. The UAE deals predominantly with direct social engineering attacks, especially through fake job offers and investment scams targeting new digital users. In Europe, while fake job scams are less prevalent, social engineering tactics such as fake banking advisors and fraudulent investment schemes are just as common as in the UAE. Additionally, fraudsters frequently leverage mule accounts for rapid fund transfers, often within the same institution, to facilitate instant payments and obscure the money trail, which presents significant challenges in both regions.

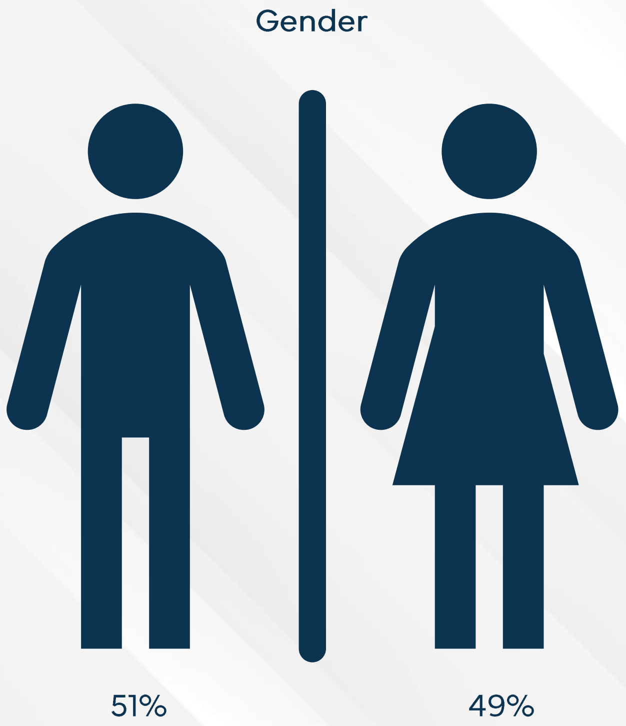
BioCatch's adaptable behavioral intelligence technology offers a solution in both of these regions by focusing on detecting manipulation and fraudulent behavior, making it an effective tool for protecting consumers as fraud tactics continue to evolve.

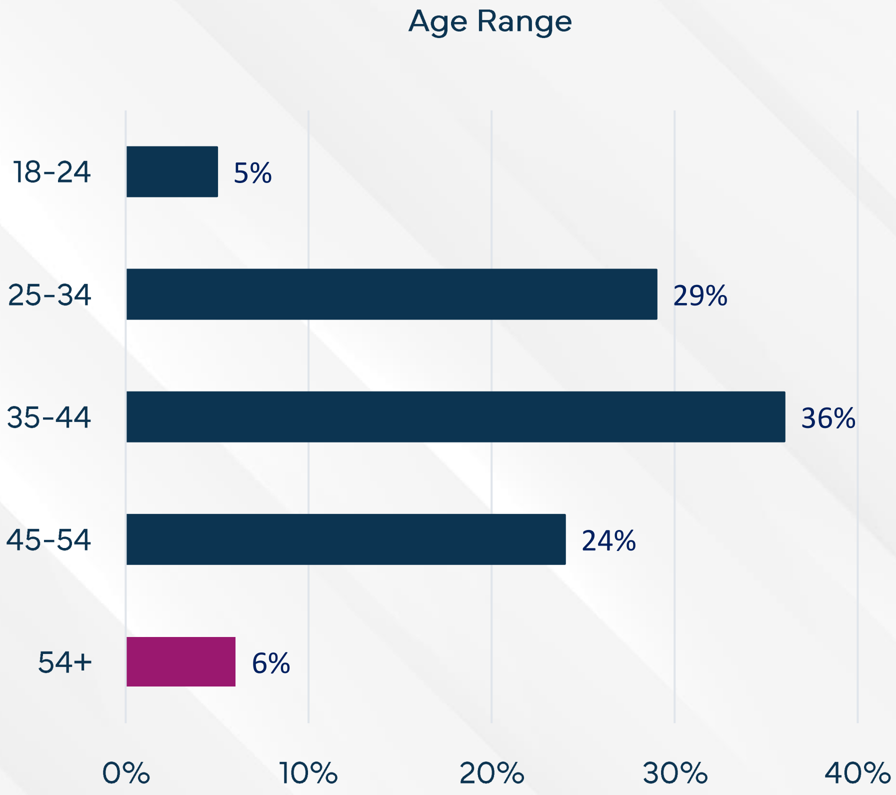
Matthew Platten, CISSP
Solution Consultant, GCC

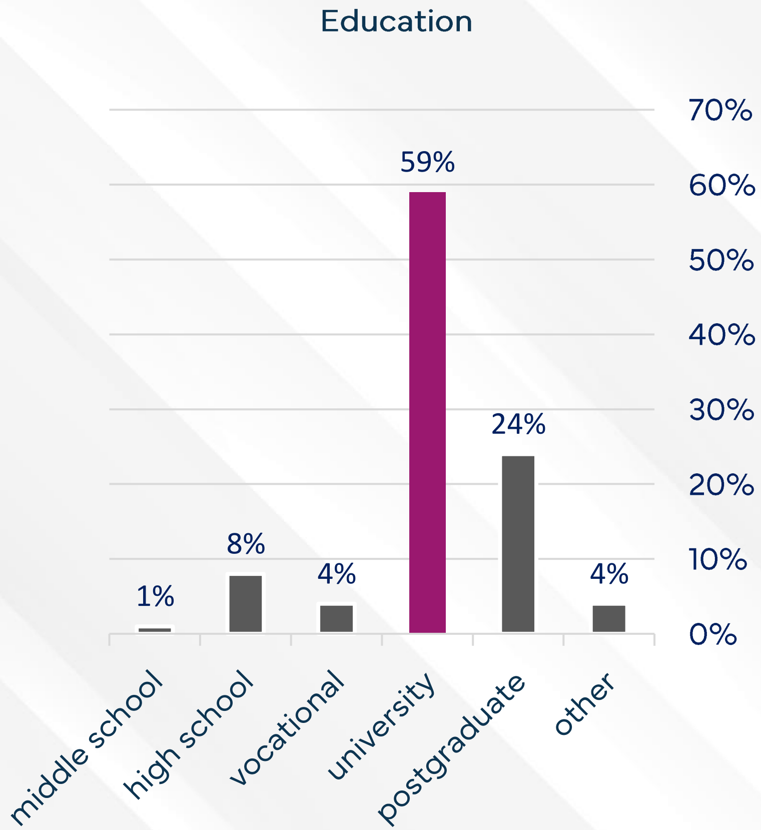
BioCatch

Ali Godrej Patel
Regional Manager, GCC

1,964 UAE citizens completed the survey





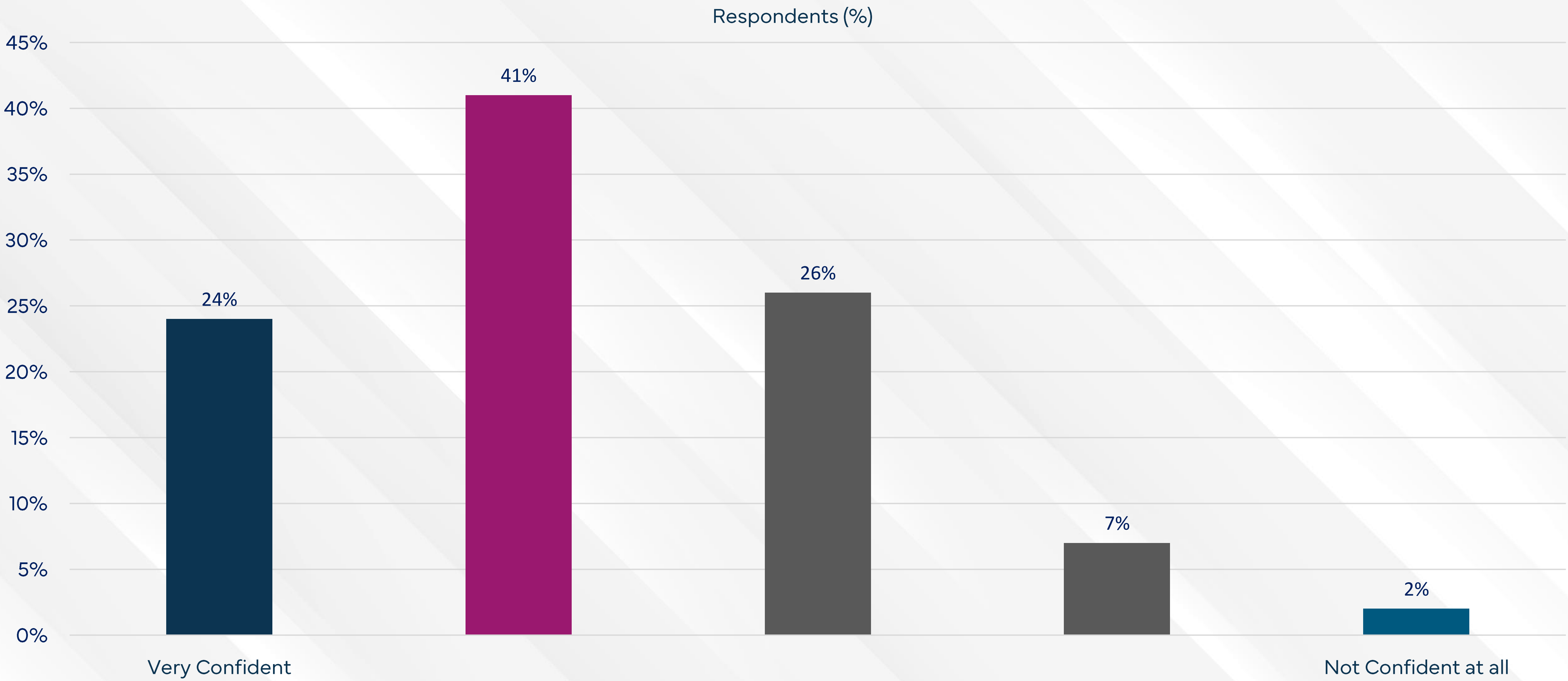


The demography of respondents to the State of Scams in United Arab Emirates 2024 survey consists to a large degree of participants with a university degree.

65% of the UAE are generally confident in their recognition of scams

BioCatch

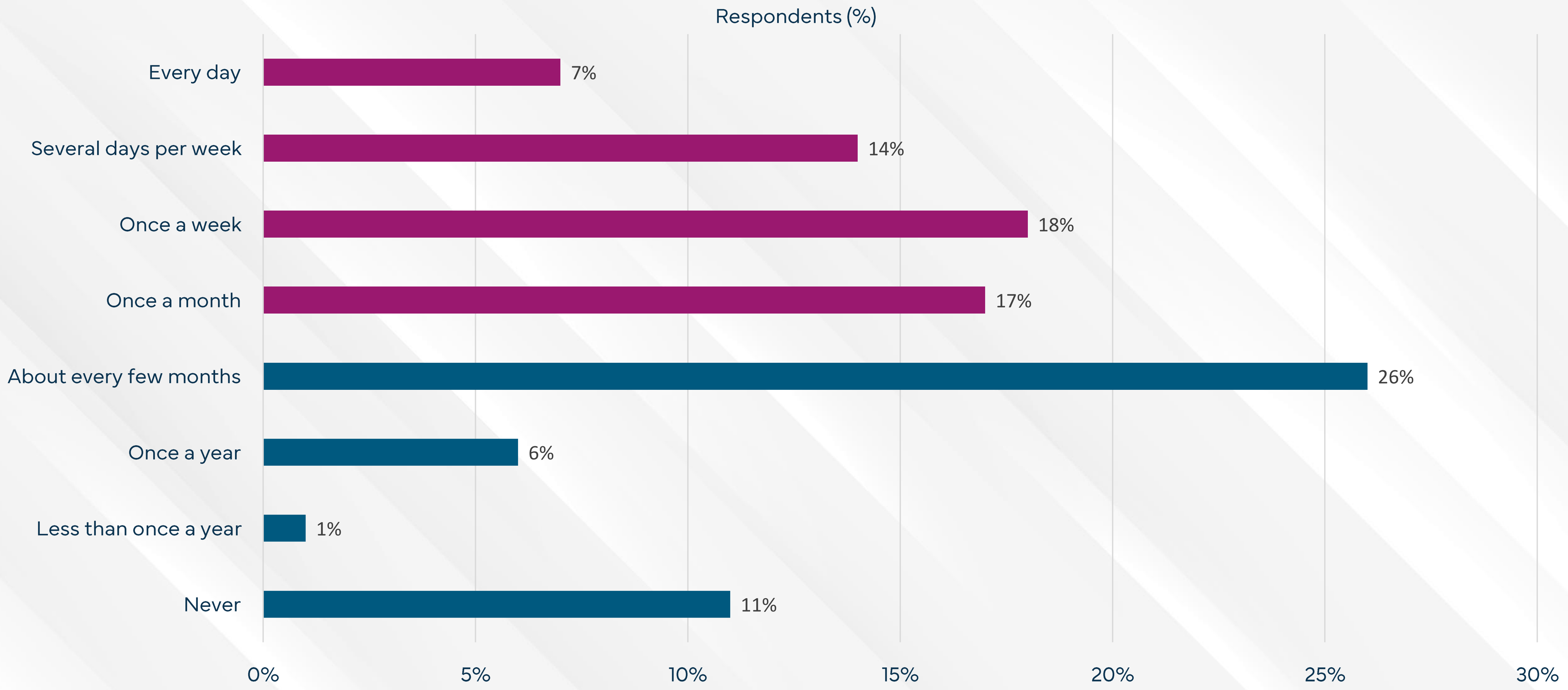
GASA
Global Anti-Scam Alliance



Only 9% of respondents do not trust in their own ability to reliably identify scams.

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

56% of the UAE population receives a scam at least once per month



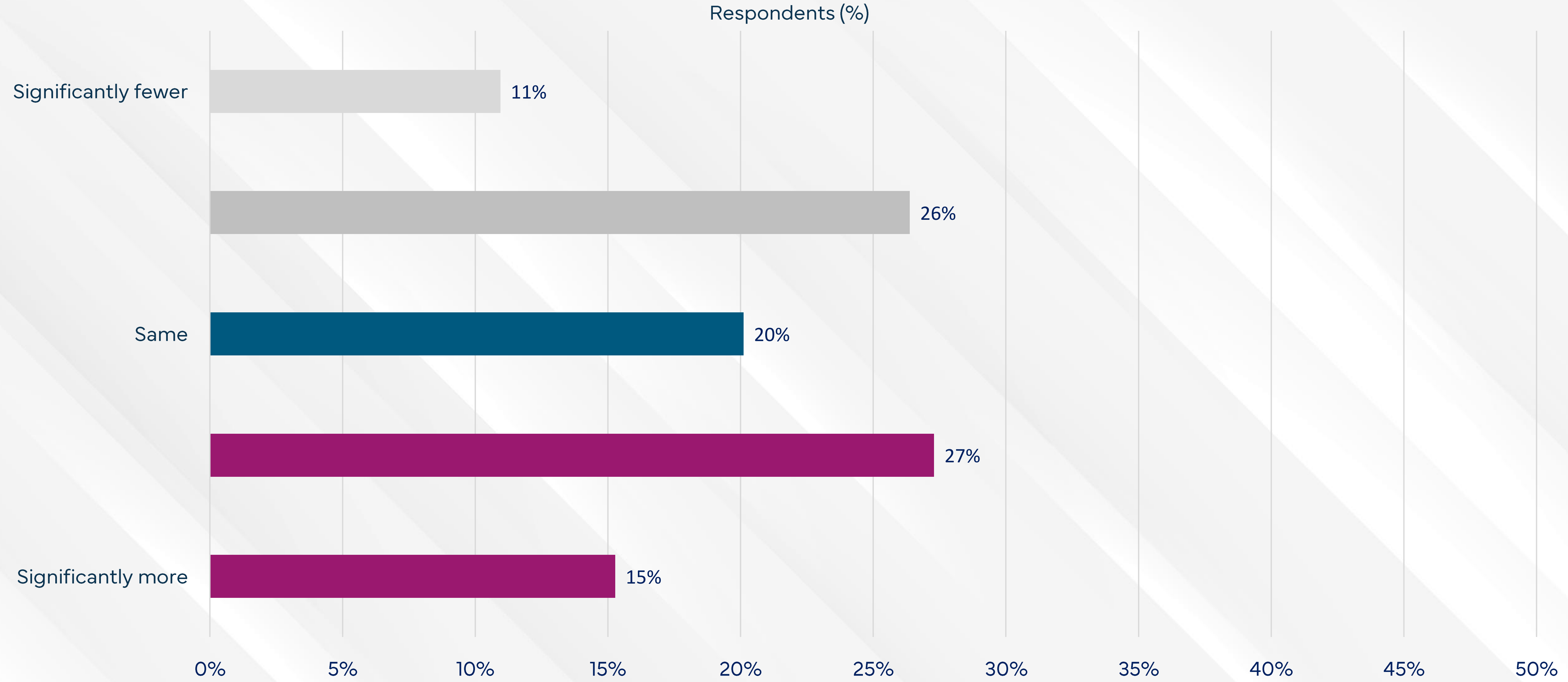
Only 12% of UAE survey respondents revealed that they are rarely confronted by scams.

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.

43% of UAE participants encountered more scams in the last year

BioCatch

GASA
Global Anti-Scam Alliance



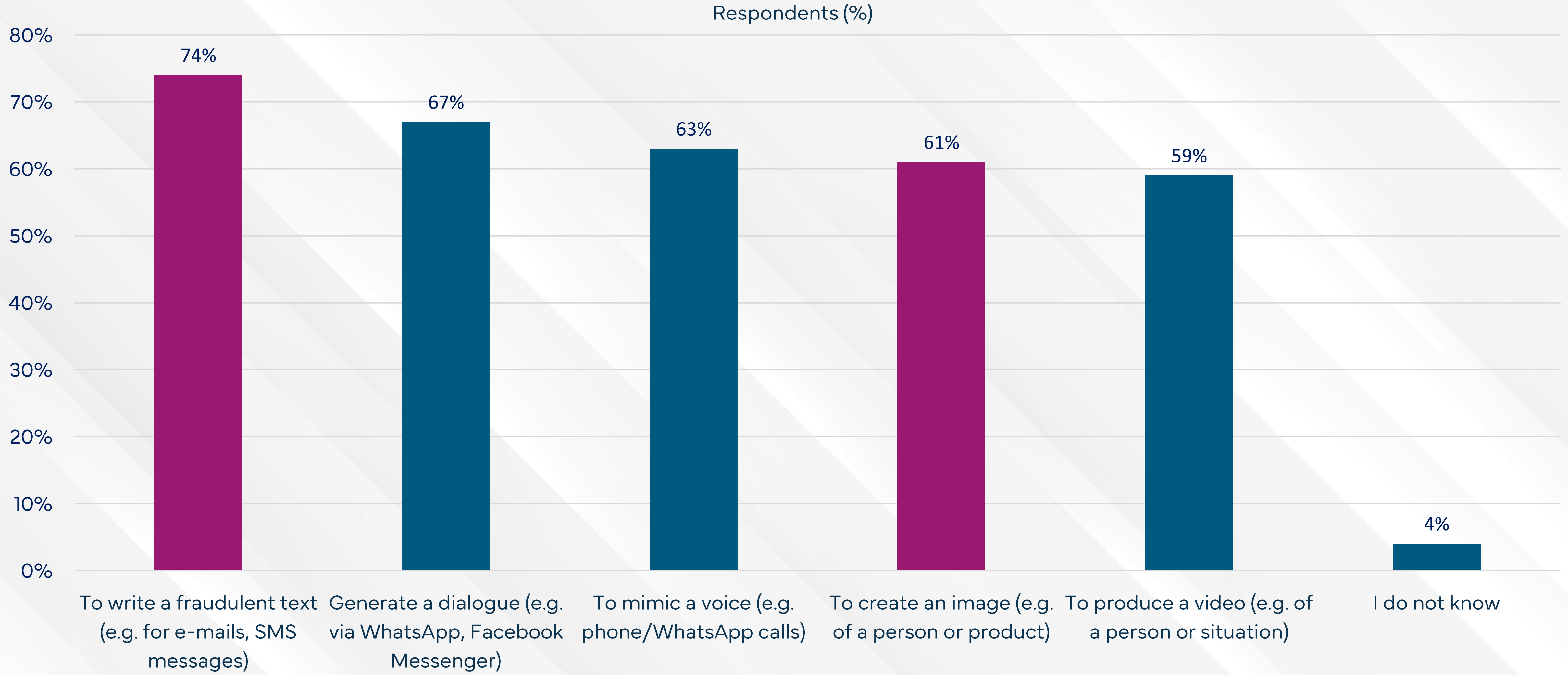
37% of UAE respondents experienced a reduction in scam encounters.

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 UAE participants are aware scammers can use AI against them

BioCatch

GASA Global Anti-Scam Alliance

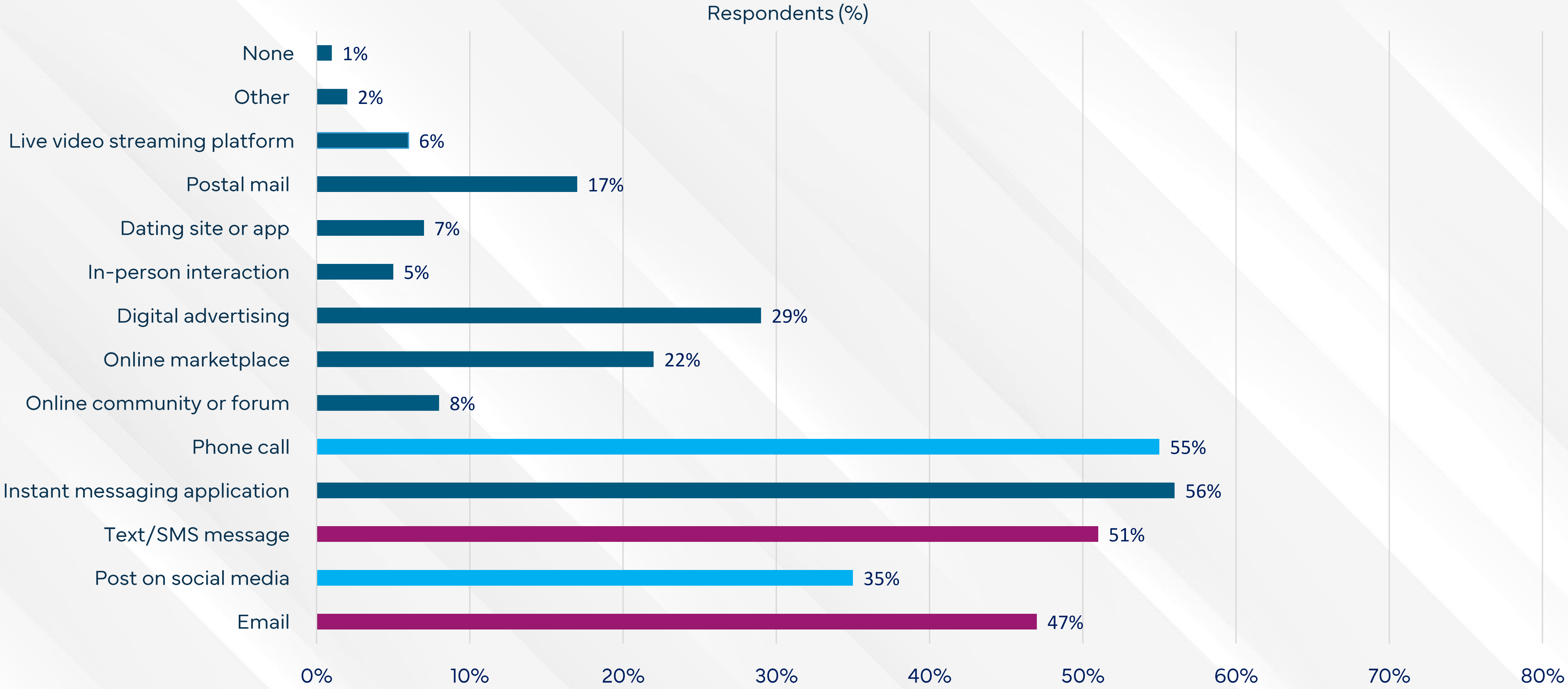


Awareness of AI generated text & images is high, with complex AI chats & videos marginally less known.

Q5 - For which of the following can Artificial Intelligence (AI) be used?

The majority of scams are delivered via Instant Messaging

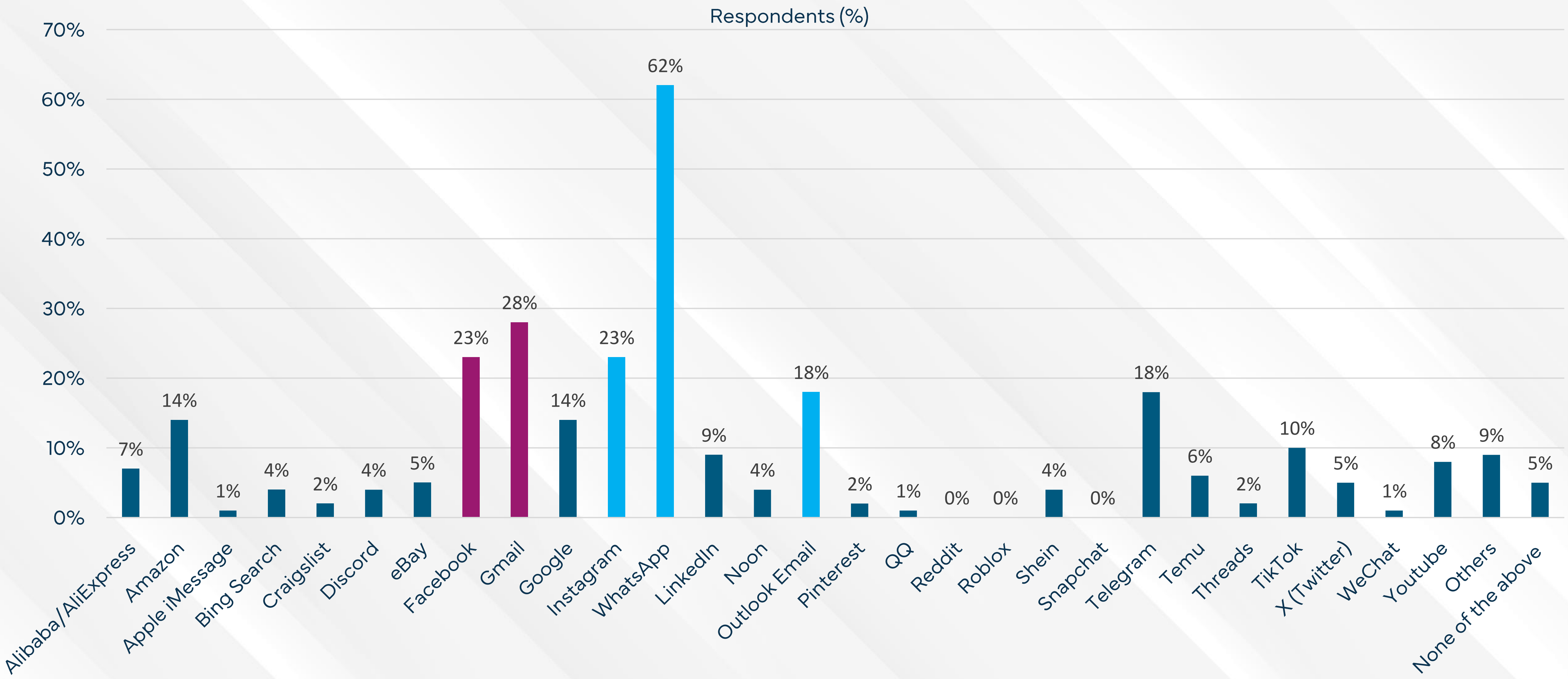
BioCatch GASA Global Anti-Scam Alliance



Phone calls and Text/SMS messages are also common scam media followed by email at the 4th place.

Q6 - Through which communication channel(s) did scammers approach you in the last 12 months? Multiple answers possible.

WhatsApp is by far the most misused as scam delivery platform



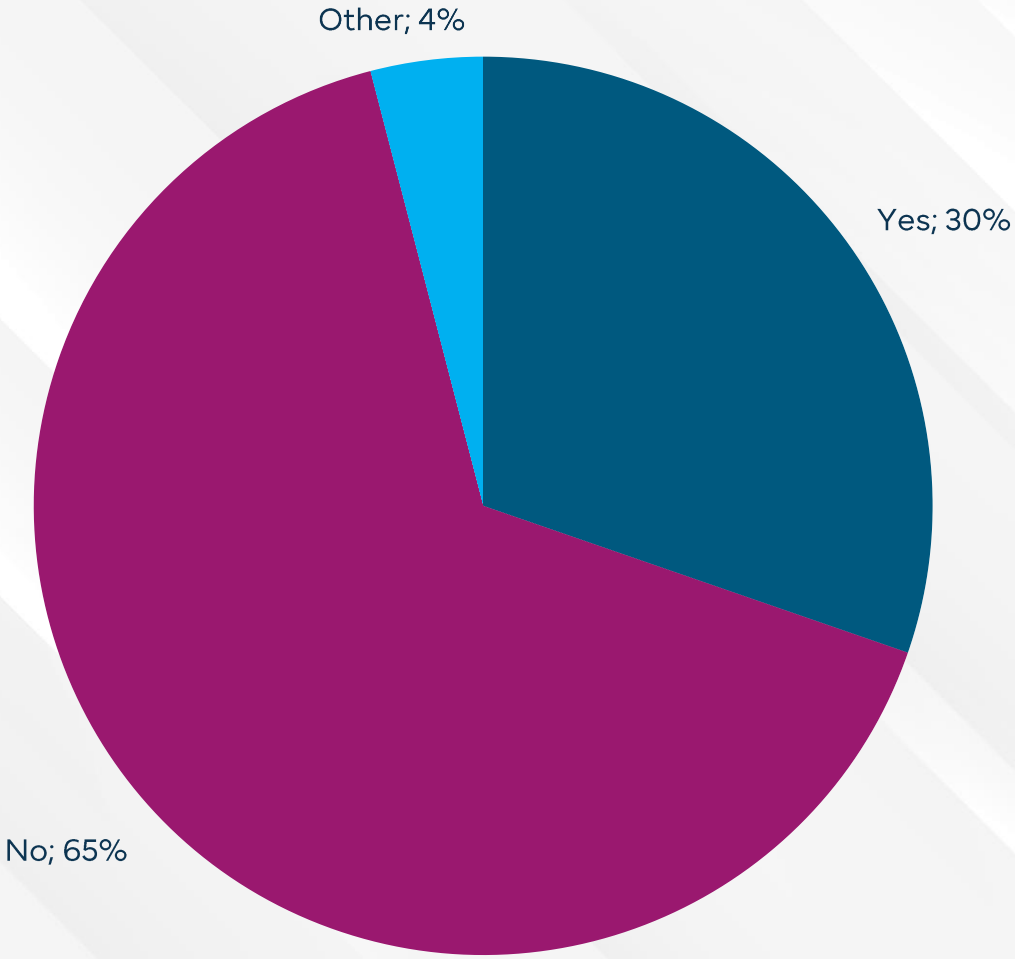
Gmail, Facebook, Instagram and Outlook round out the top five most popular platforms for scammers.

Q7 - Though which platform(s) did scammers contact you in the last 12 months? Multiple answers possible.

65% of the UAE victims did not report the scam to law enforcement

BioCatch

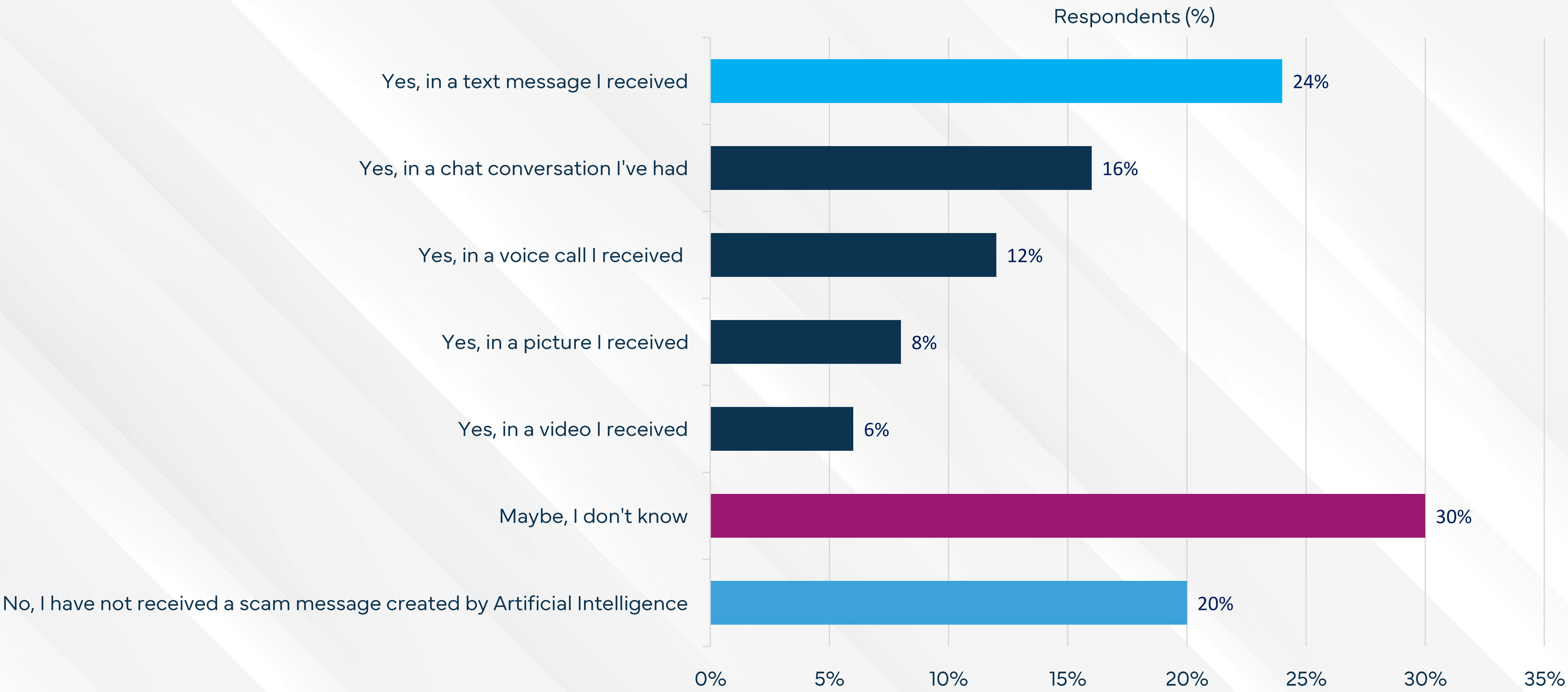
GASA Global Anti-Scam Alliance



30% 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?

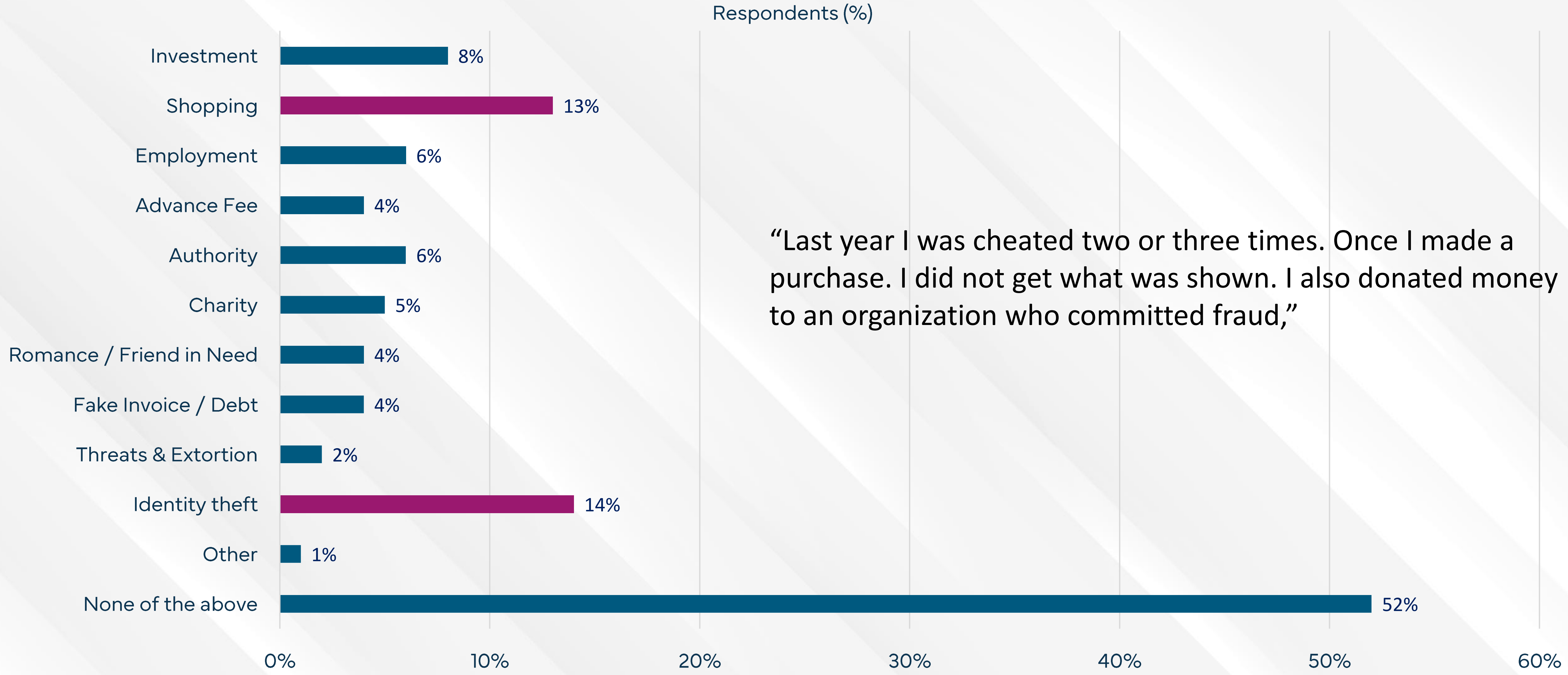
30% of UAE respondents were uncertain whether AI was used



20% of the UAE 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? Multiple answers possible.

Shopping Scams & Identity Theft are the most common scam



"Last year I was cheated two or three times. Once I made a purchase. I did not get what was shown. I also donated money to an organization who committed fraud,"

1.77 scams were reported per victim, suggesting that scam victims are likely to be retargeted.

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

Hear the stories shared directly from UAE scam victims

“I bought a ticket online and never received it.”

“ An estate agent who scammed me and my husband out of a first rental payment for an apartment.”

“I received a call asking for my personal information such as my Emirates ID. Some amounts have been deducted from my credit card afterwards.”

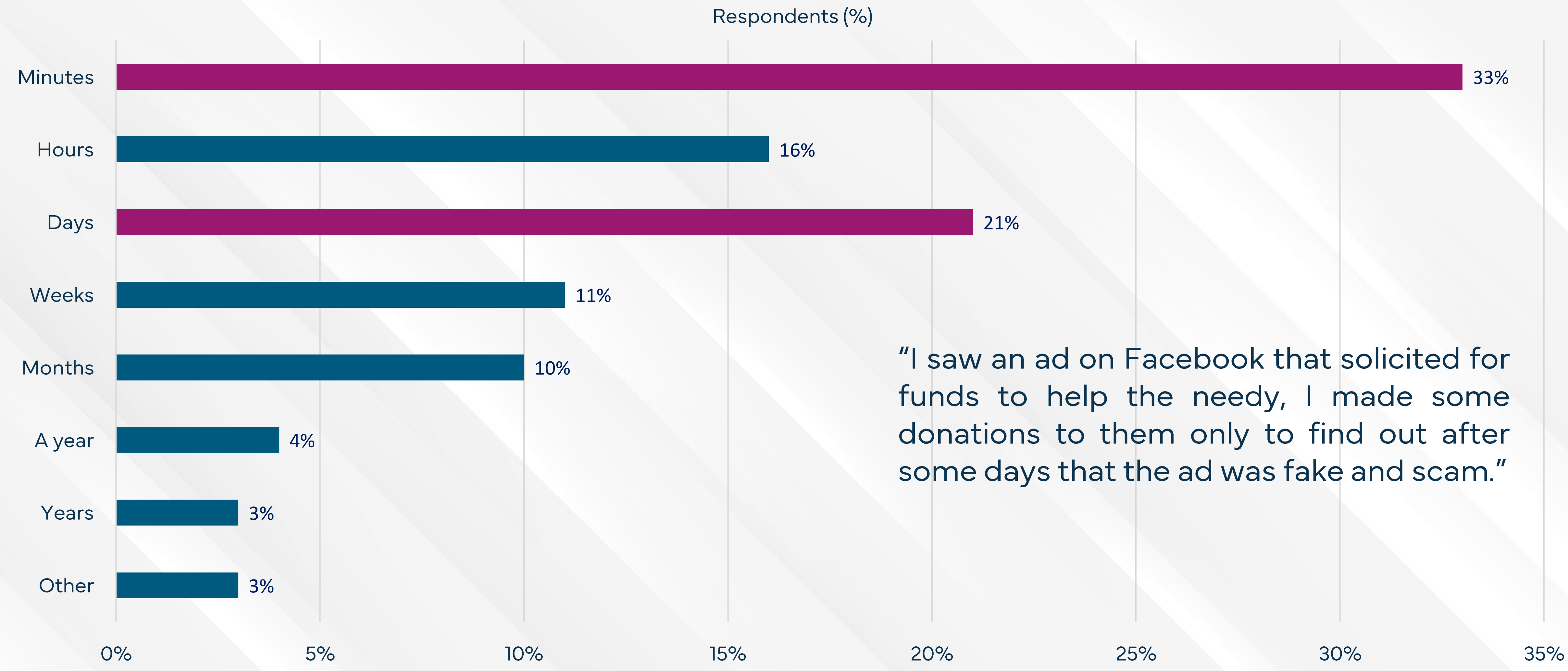
A brand images of Desi Ghee were used in Facebook advertisement by some fraud person and he tricked me to pay for a product.

“People called me and said they are from the police and asked to provide them with a one-time password send to me.”

“I started an online job completing task. Then they convinced me to invest a huge amount. My money is now gone.”

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

BioCatch GASA Global Anti-Scam Alliance

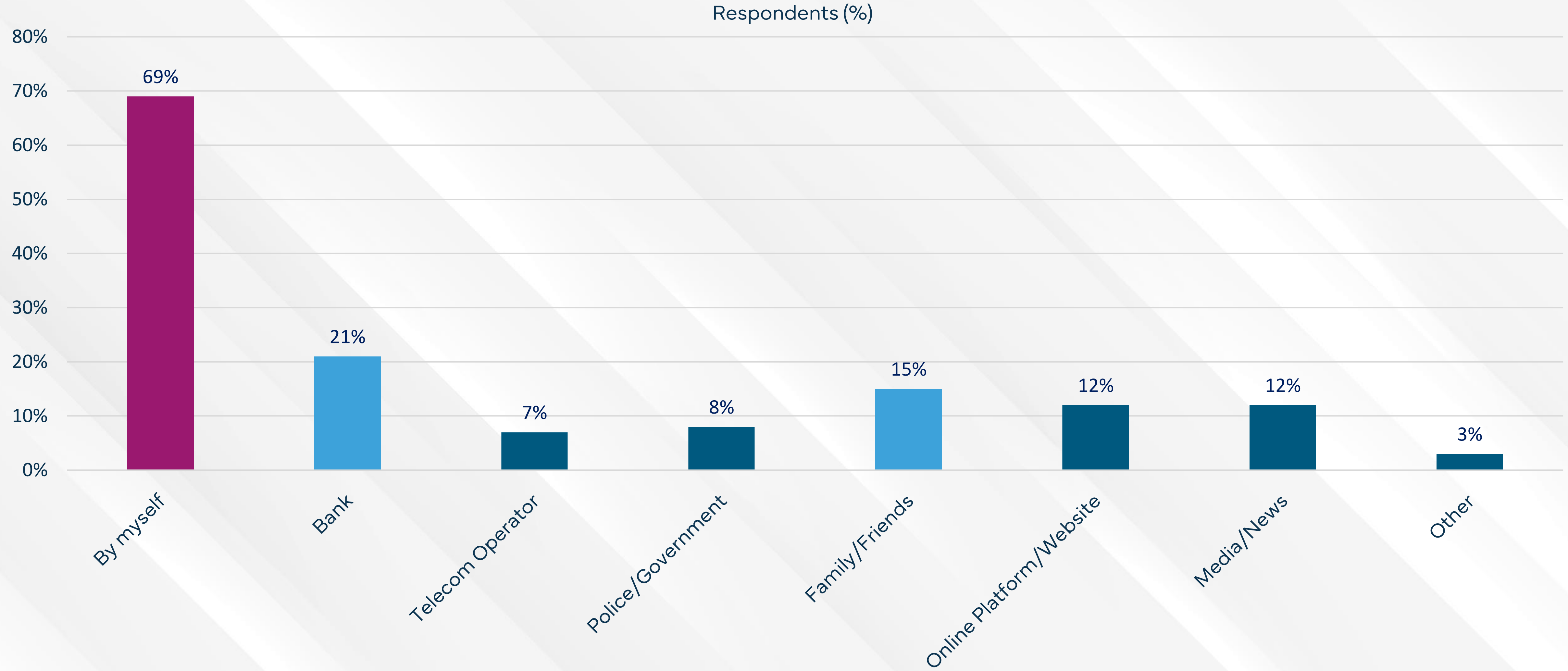


> “I saw an ad on Facebook that solicited for funds to help the needy, I made some donations to them only to find out after some days that the ad was fake and scam.”

33% were scammed in a matter of minutes, but 7% were targeted with a long con of 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?

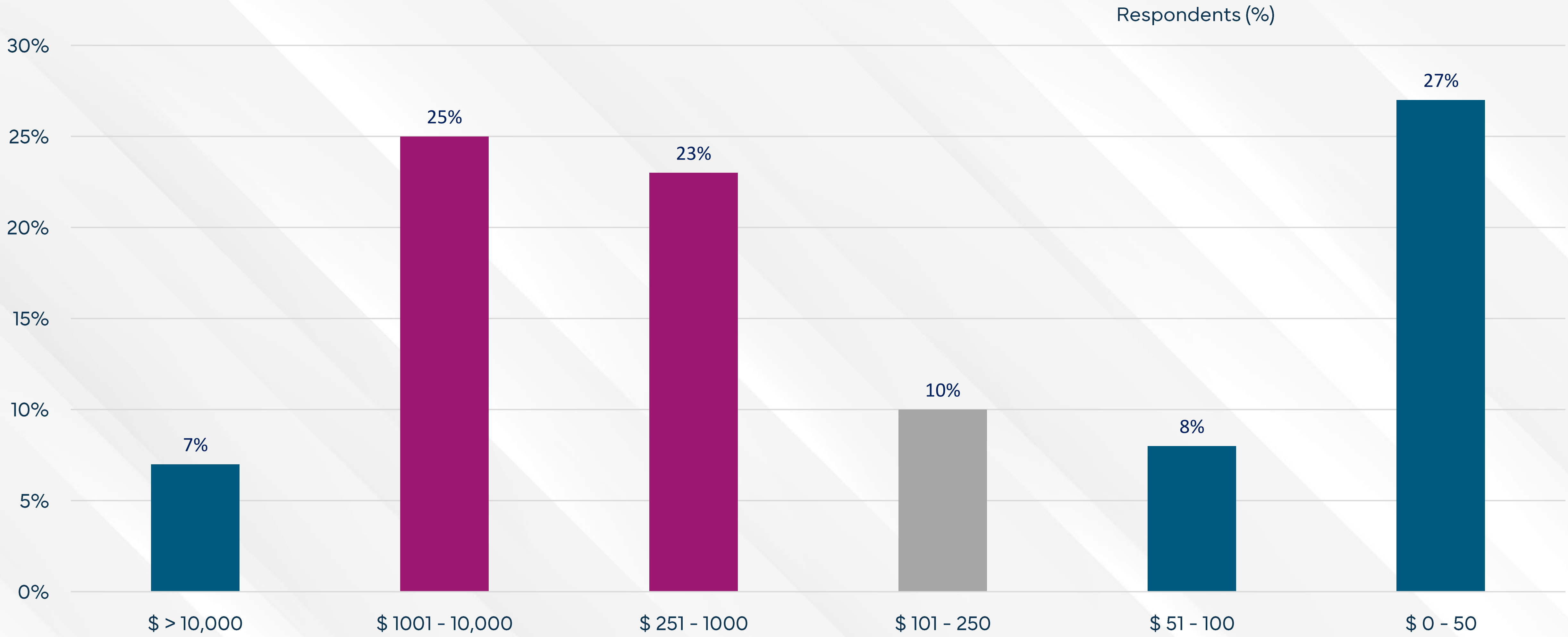
69% came to their own conclusion that they had been scammed



21% were notified by banks, while friends/family are also popular in pointing out scams.

Q13 How did you discover you were scammed?

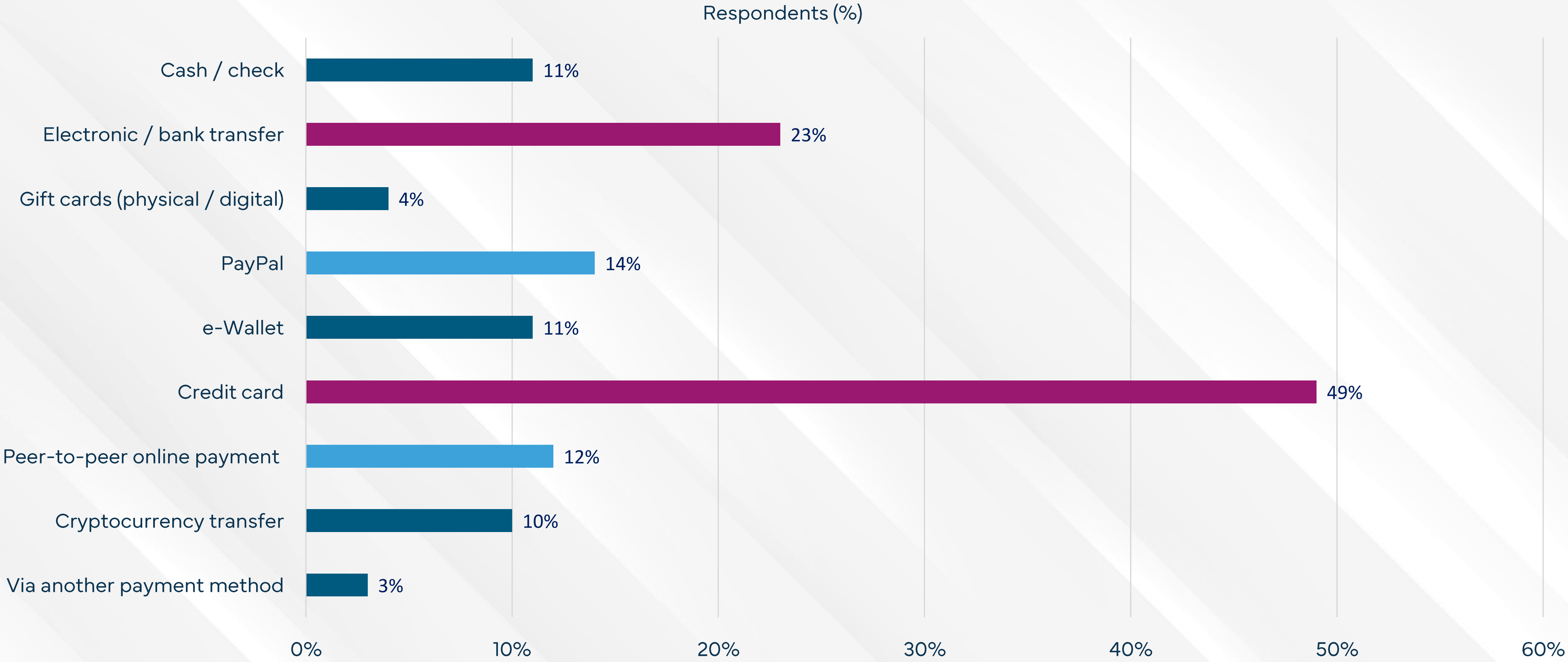
In total, 27% of UAE survey participants lost money to a scam



The average amount lost in US dollars by the victims was $ 2,194 with several victims reporting loses over $ 50,000

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

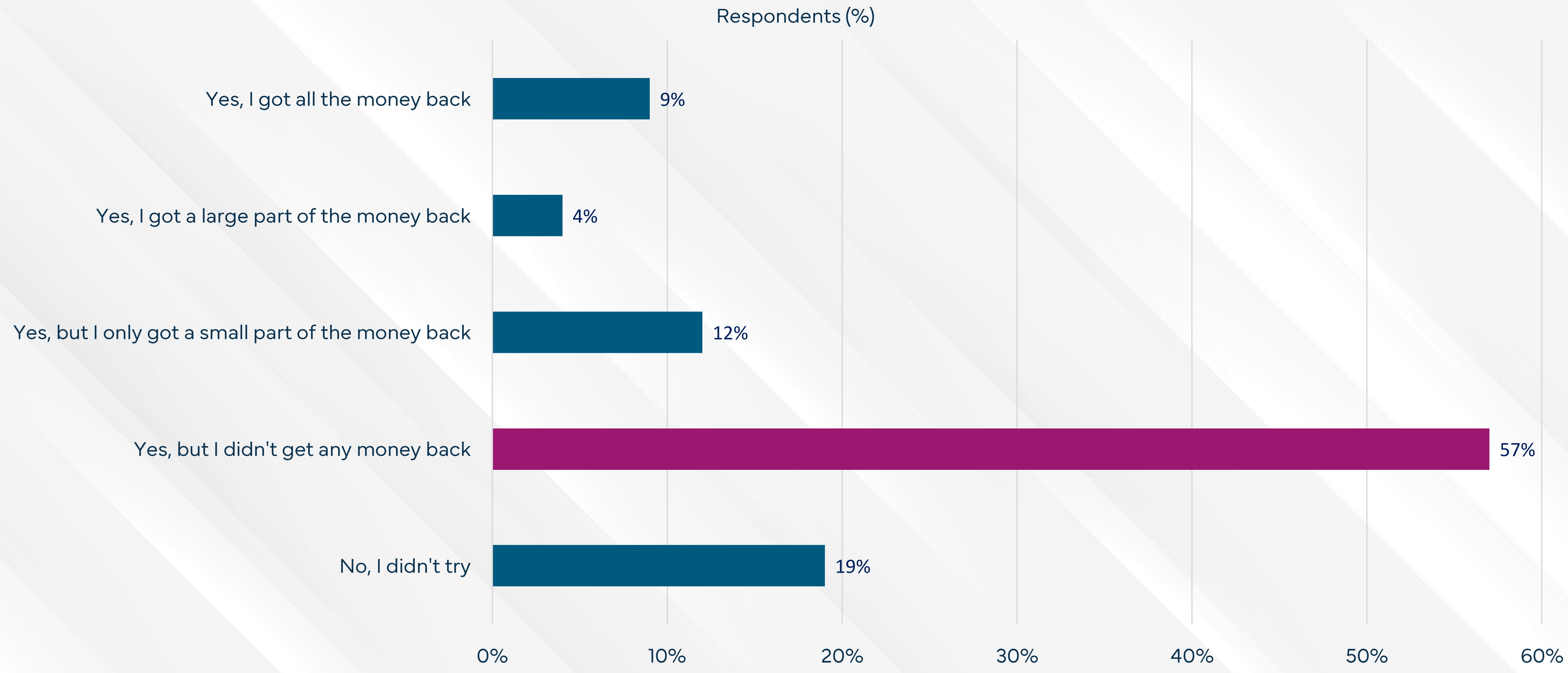
Credit Cards & Bank Transfer are the top scam payment methods



PayPal and peer-to-peer apps are also popular tools which scammers use to collect stolen funds.

Q15 - How did you pay the scammer? Multiple answers possible.

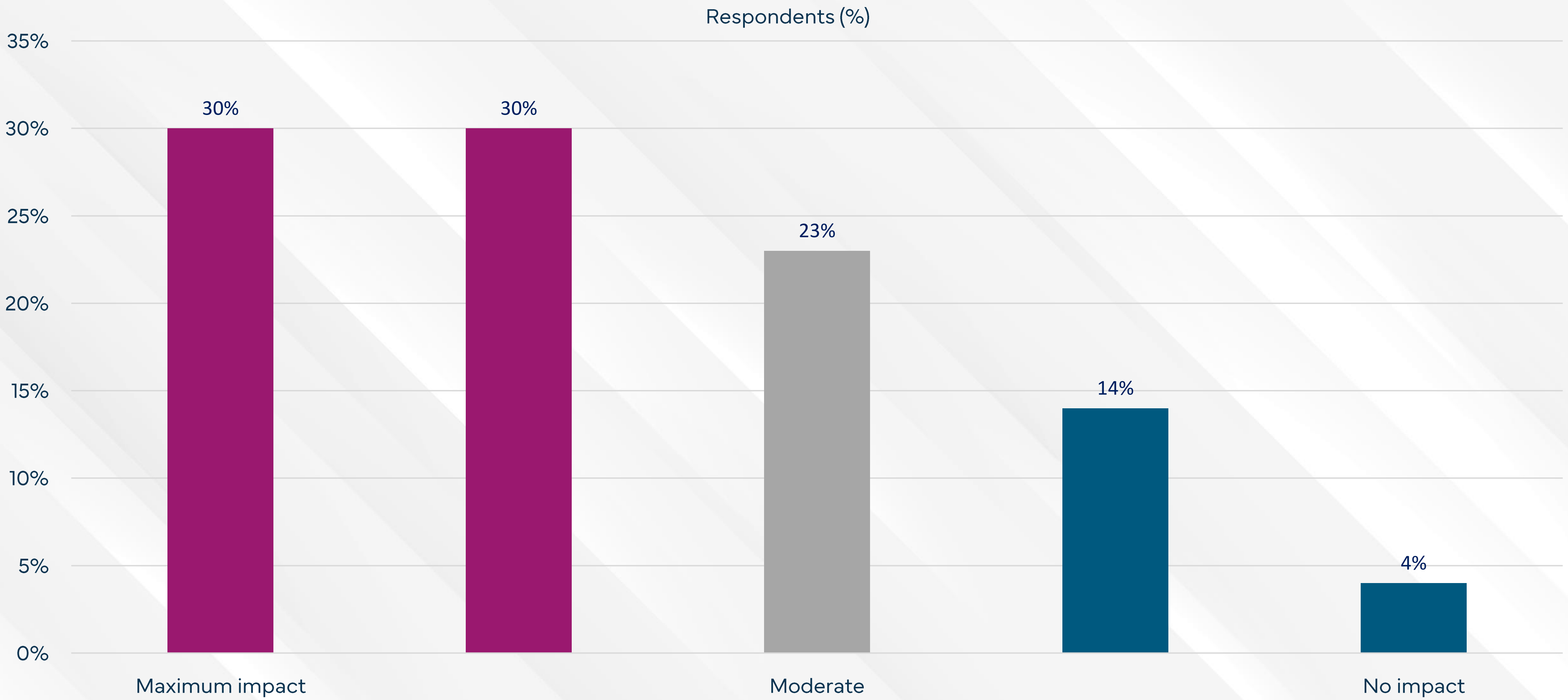
Only 9% of victims were able to fully recover their losses



19% did not try to recover their funds. 57% tried but were not able to recover any money.

Q16 – Did you try to recover the money lost?

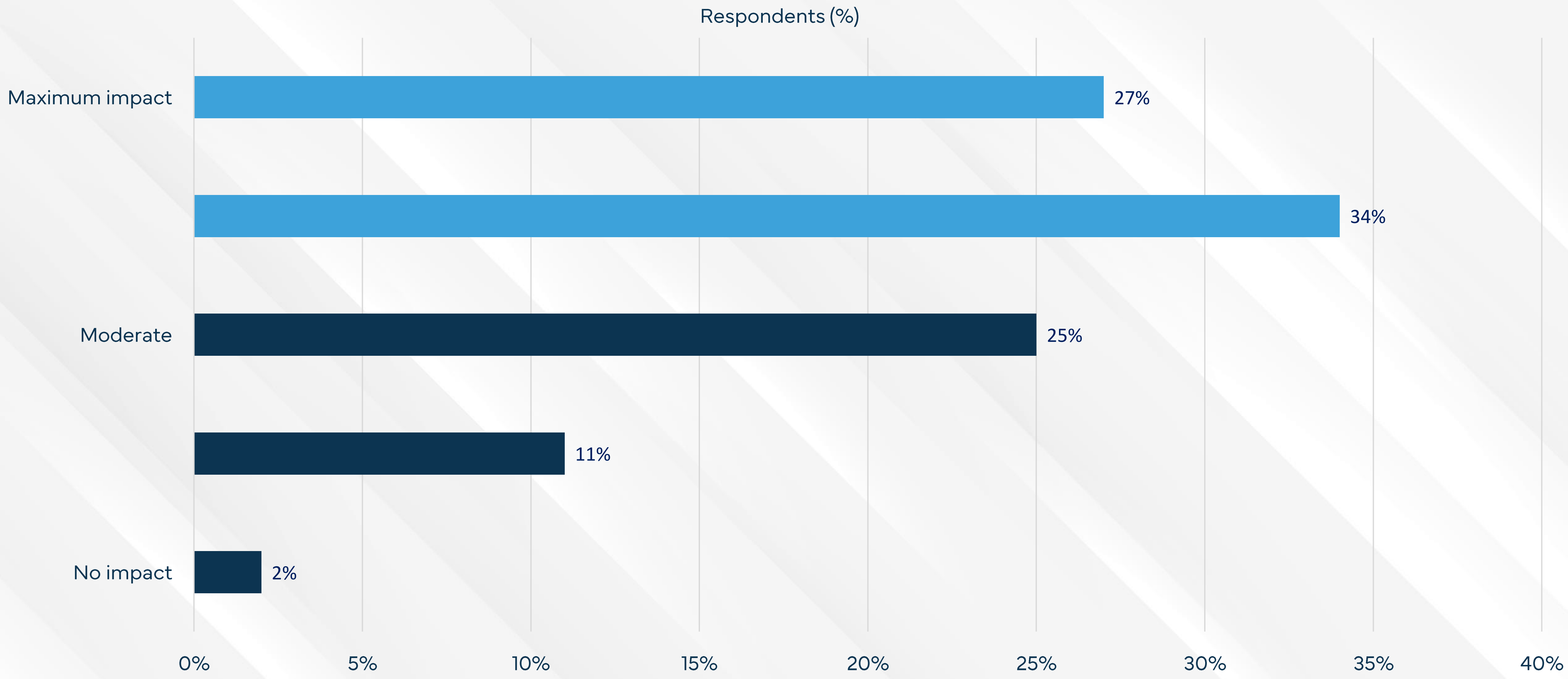
59% of UAE victims perceived a strong emotional impact



18% of the survey respondents reported little to no emotional impact due to scams.

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

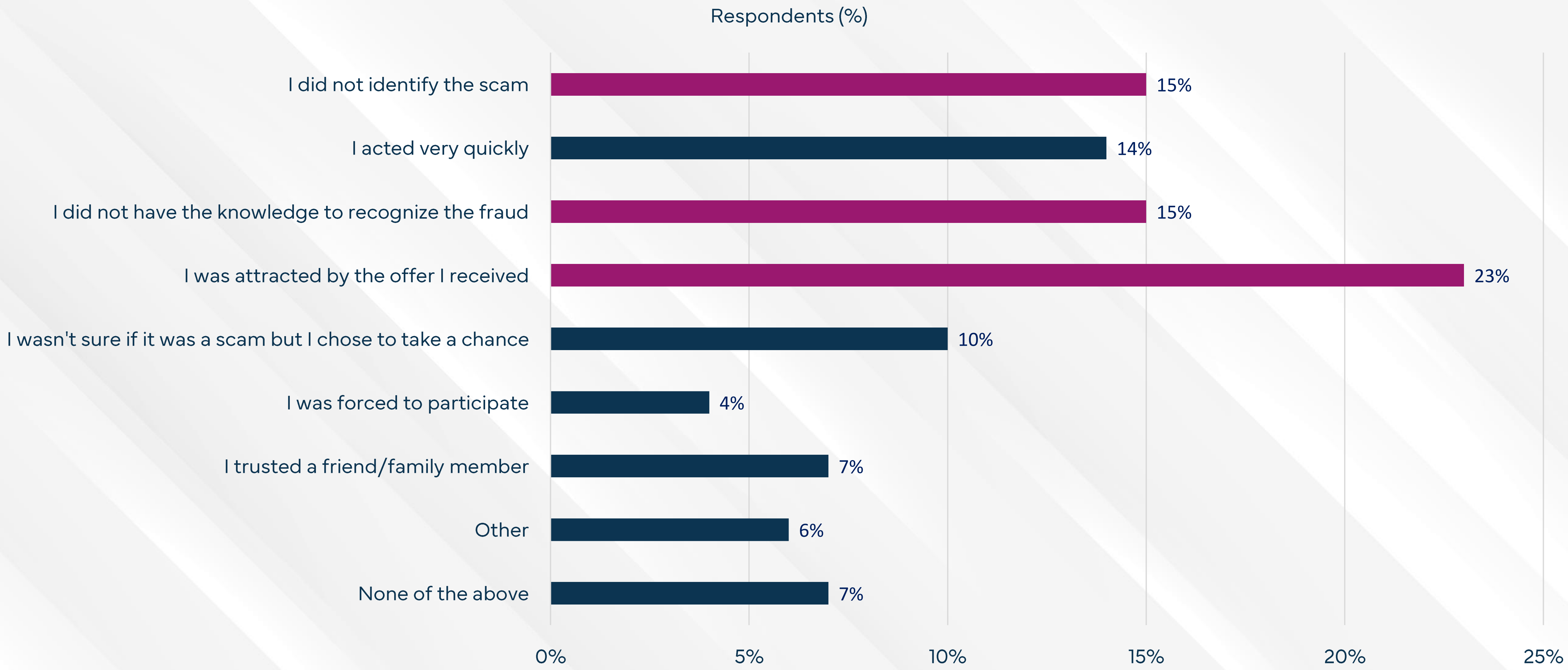
62% of the UAE panel have less in trust the Internet due to scams



13% of the UAE 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?

Most UAE victims were attracted by the offer of the scammer



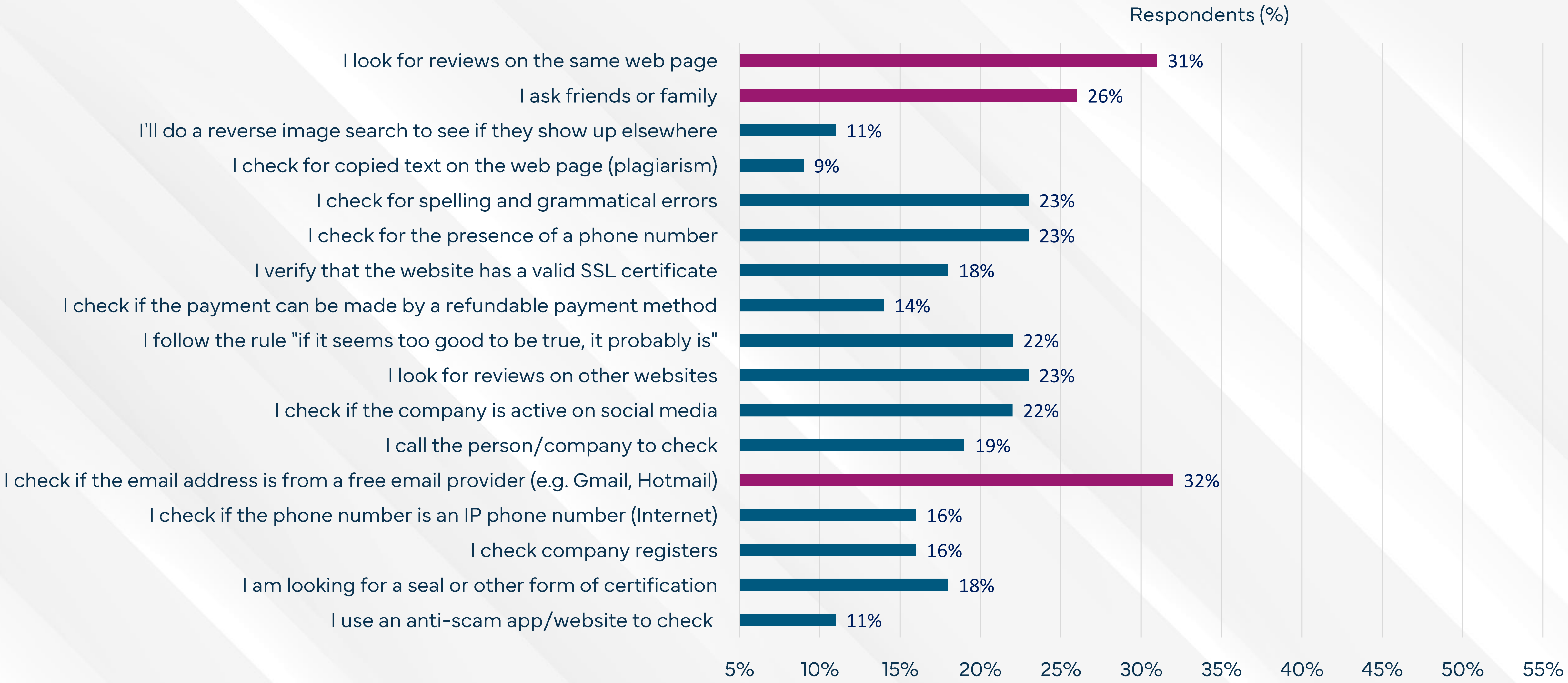
A sizable portion also reported they did not detect the scam until it was too late or lacked the knowledge.

Q19 - What was the main reason you were deceived?

Most respondents check the email address and review sites

BioCatch

GASA Global Anti-Scam Alliance



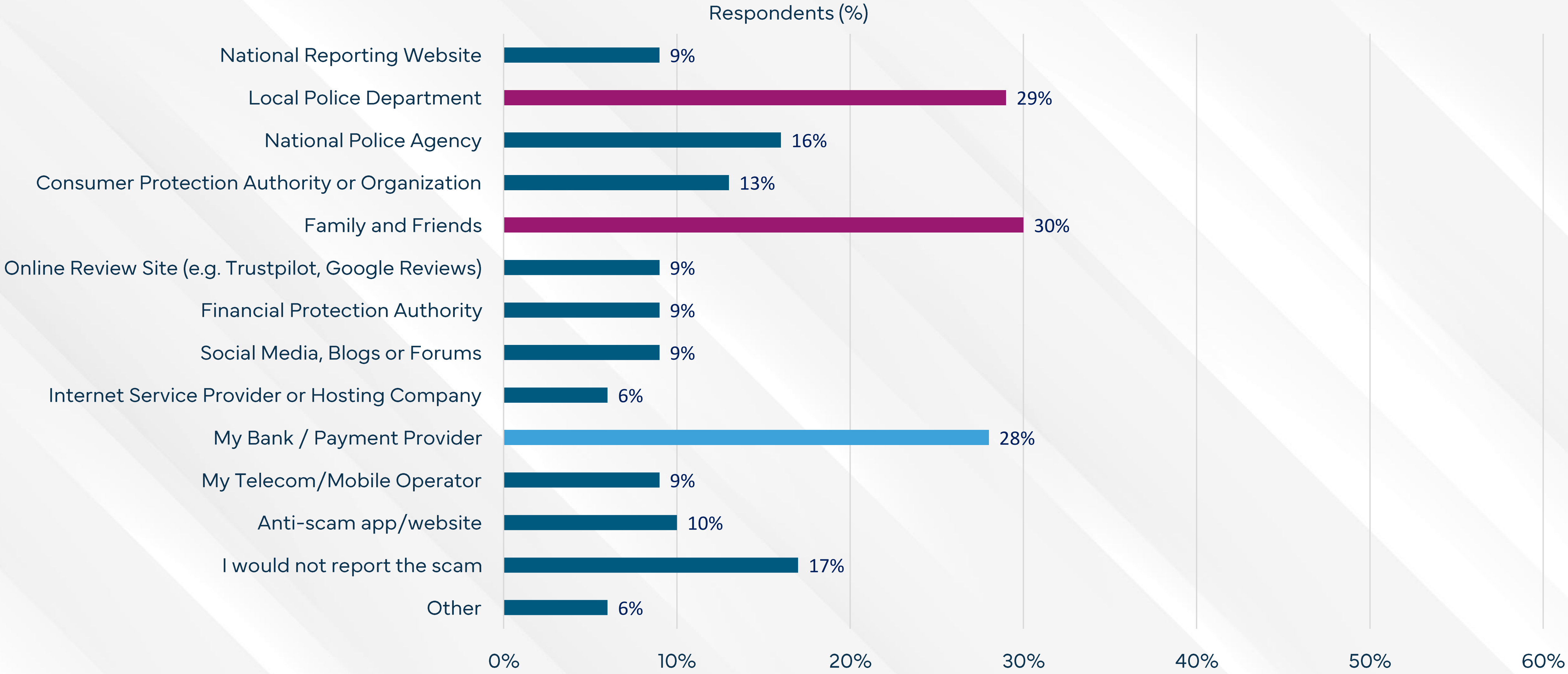
Other ways to check if a website is real or a scam are asking friends & family.

Q20 - What steps do you take to check if an offer is real or a scam? Multiple answers possible.

Scam experiences are mostly shared Family & friends & local police

BioCatch

GASA
Global Anti-Scam Alliance

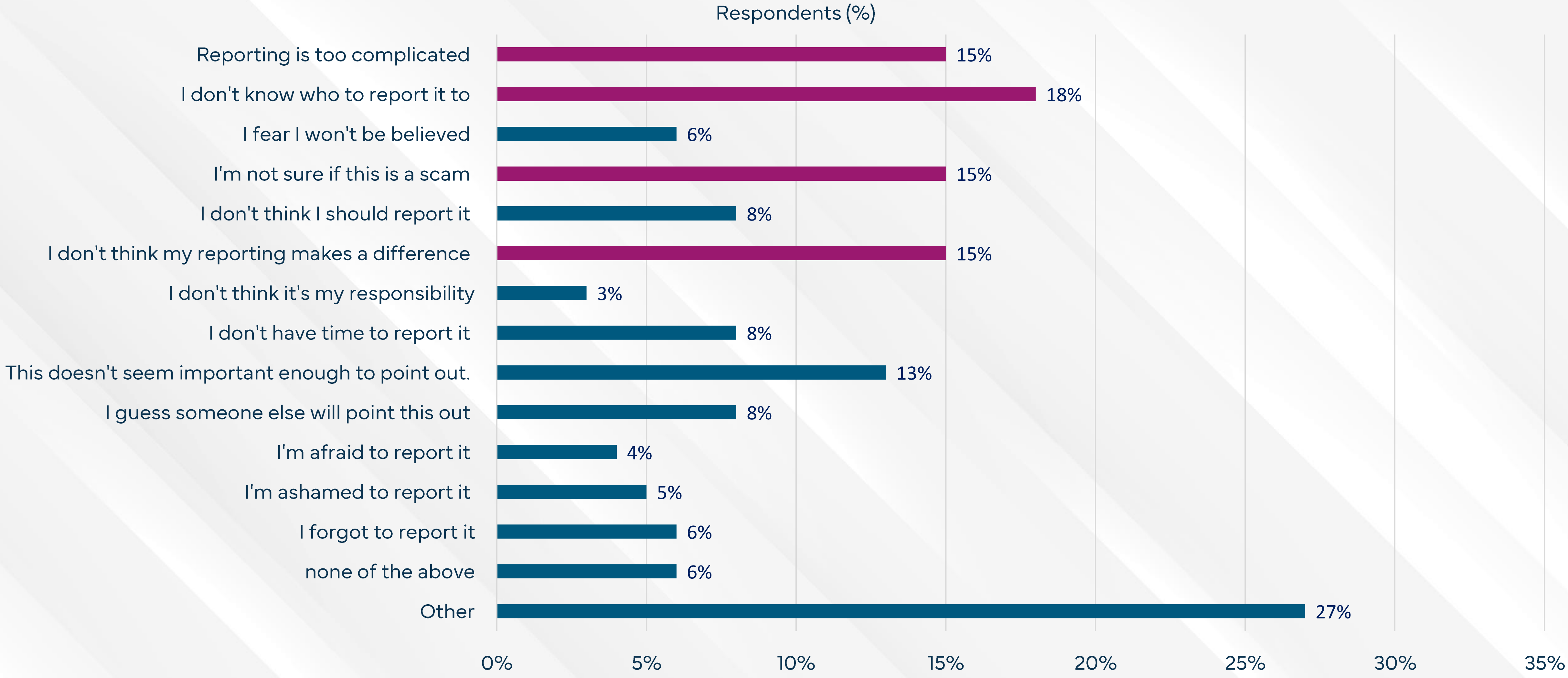


Banks & payment providers are the third place to report scams

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

Many UAE participants do not know who to report the scam to

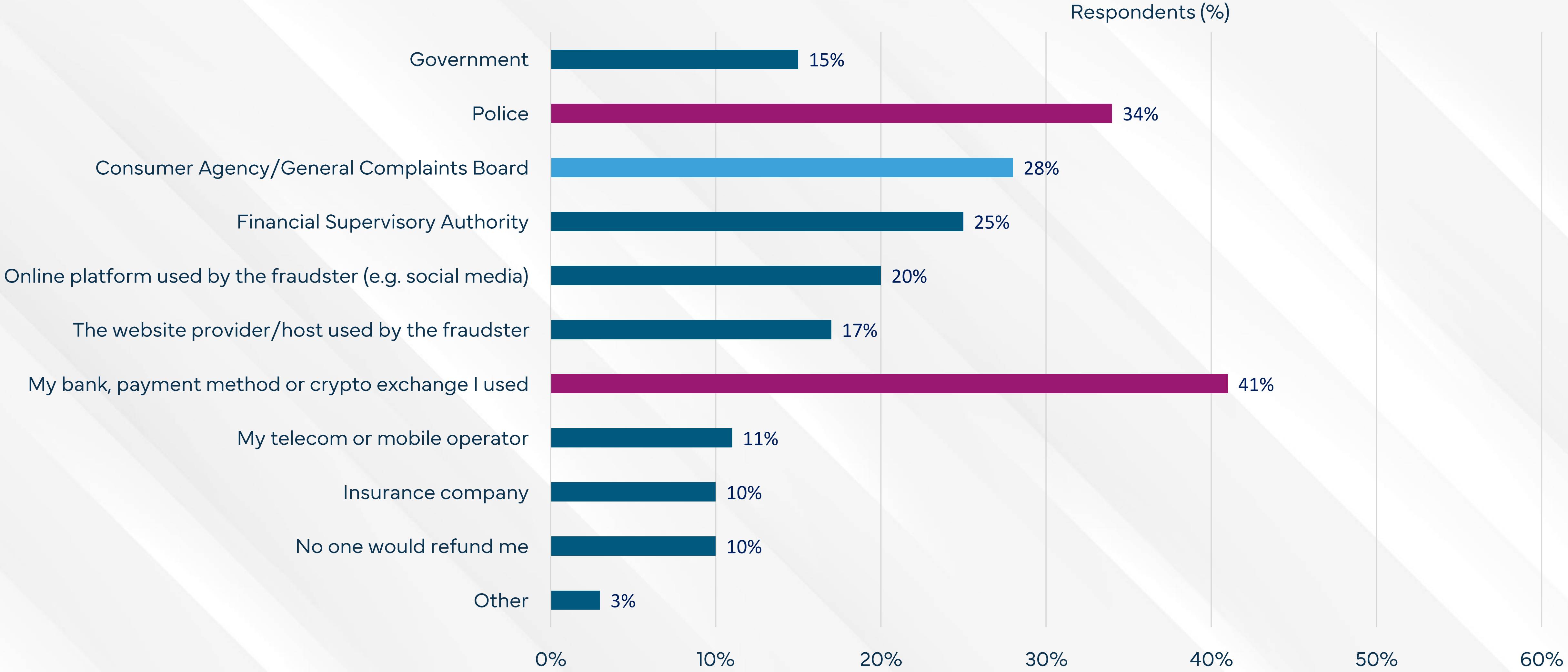
BioCatch GASA Global Anti-Scam Alliance



Other reasons not reporting are the complicated process, scam uncertainty and not making a difference.

Q22 – What reasons might you have to not report a scam? Multiple answers possible.

10% of the UAE panel assume no one will refund their scam losses

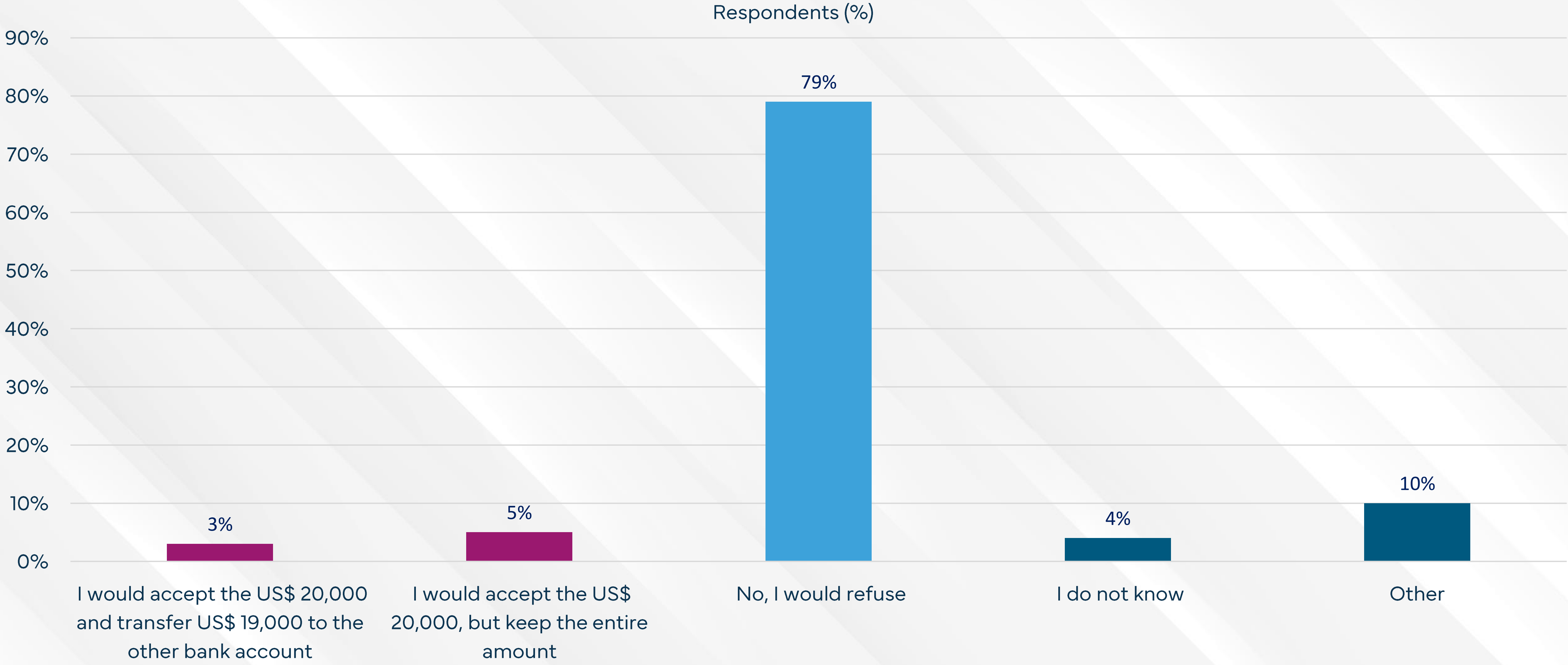


Others believe their bank, the police or consumer protection agency will refund them.

Q23 – If you were scammed, who do you think should be responsible for making sure you are paid back for your loss? Multiple answers possible.

8% of UAE respondents would consider being a money mule

BioCatch GASA Global Anti-Scam Alliance



However, 79% of those surveyed claim they 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.

TRENDS Research & Advisory is an independent research institution that aims to contribute to the shaping of the future. It analyzes the geopolitical, economic, and social aspects of regional and global developments in order to better understand the various dimensions of prevailing trends and the opportunities and challenges they present, while adhering to international standards in research.

BioCatch helps the largest and most recognized financial institutions and telecommunications brands establish trust with their customers, while protecting them from digital fraud. As behavior has become one of the few elements of our digital identities that is truly and uniquely human. By leveraging these behavioral factors, BioCatch provides its clients with powerful and reliable analysis to ensure the authenticity and integrity of transactions.

Methodology

1. Survey Administration:

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

2. Incentives and Fraud Prevention:

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

3. Data Correction and Estimation Challenges:

- **Statistical Corrections:** Adjustments made based on the general demographic distribution within each country to account for potential biases in age or education level.
- **Estimation Limitations:** Outliers were removed as needed, and losses under one bitcoin were not included due to reporting constraints.

4. Additional Data Sources:

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

5. Translation and Localization:

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

6. Inspirational Reference:

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

About the authors

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

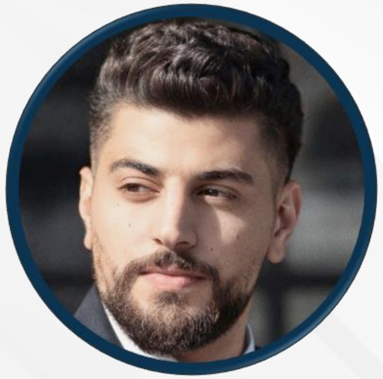
Nowadays, Jorij is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.

Sam Rogers is GASA's Director of 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 contributing something worthwhile to society.

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.



Ammar R. Al-Amarneh is an Opinion Poll Senior Specialist with extensive experience in statistical analysis and field research development. He currently holds this position at the TRENDS Research and Advisory Center, where he leads the design and implementation of surveys aimed at providing strategic insights for decision-makers.

He holds a Master's degree in Applied Statistics from Yarmouk University.

Serhat S. Çubukçuoğlu is a Senior Researcher in Strategic Studies at TRENDS Research & Advisory in Abu Dhabi, UAE. Previously, he worked in software engineering and technology business before transitioning into a career as a geopolitical strategist specialized on the intersection of policy analysis, consultancy, and academia. Serhat frequently appears on media both as a commentator and a moderator, reflecting on the ongoing politico-economic developments and strategic discussions in the Middle East.

Adel Nabhan ElNaggar is a seasoned business analyst and project manager with over 14 years of global experience. He is currently Projects Manager at Trends Research and Advisory in Abu Dhabi, leading multi-million-dollar projects across industries. With expertise in international relations, project management, and economic development, Adel focuses on strategic planning.

Previously, he managed EUR 160 million programs at the European Union Delegation to Egypt.

Disclaimer

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

Copyright

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. The authors permit 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 (Twitter): @ScamAlliance
LinkedIn: linkedin.com/company/global-anti-scam-alliance