SCAMADVISER

The Global State of Scams - 2023

GASA
Global Anti-Scam Alliance

25.5% of global population defrauded as $1.026 trillion is stolen by scammers

In the increasingly unpredictable digital age, the annual Global State of Scams report, a collaborative effort by the **Global Anti-Scam Alliance (GASA) and ScamAdviser**, meticulously details the interconnected world's vulnerability to fraud. The comprehensive survey involved the experiences and insights of **49,459 individuals from 43 countries**, providing diverse perspectives on the multifaceted world of scams. While diverse, the survey participants' demography leans notably towards males, particularly in the case of developing countries, primarily aged 35–44 with a university degree.

A significant **69% of global participants express confidence in recognizing scams**, showcasing a broad self-assuredness in scam identification across the world. Contrarily, a substantial **59% of individuals worldwide still face encounters with scams at least once a month**, marking a stark contrast between **self-perceived awareness & actual vulnerability to scams**.

Worldwide, an alarming **78% of participants experienced at least one scam in the last year**. With a dominant occurrence of **shopping scams (27%)**, followed by **identity theft (21%)** and **investment fraud (20%)**, the report highlights a **universal vulnerability** to these scam types. **Phone (61%)** and **text/SMS messages (58%) are still the leading channels for scam attempts** worldwide, indicating a universal preference for these mediums by scammers.

Attractive offers emerge as the predominant lure. This was the sadly the most common factor in developing countries such as **Pakistan, Indonesia (34%), Egypt, Kenya, India, Nigeria & South Africa (all 33%)**. However, **not identifying the deceit** or **lacking the knowledge to recognize the scam** take a close second and third place. Victims in developed nations like **Taiwan (30%), France (27%) & South Korea (26%) often reported that they didn't identify the situation as a potential scam**.

A pattern of revictimization emerges, indicating a global phenomenon of scammers returning to their prey to victimize them again. Most countries experience a **revictimization rate of 1.5 per person**. At the extreme end of the scale, **Kenyans (3) and Nigerians (2) are retargeted the most**.

There is **a tendency (by 59% of respondents) towards not reporting due to perceived complexity and uncertainty**, highlighting a worldwide challenge in scam reporting and resolution. This is somewhat unsurprising, considering the varying confidence in authority efficiency and effectiveness. **24% simply do not report because they believe that doing so will achieve nothing**. With public frustration at the lack of arrests following scam reports topping the list of grievances, **Brazilians and Thais regard their authorities as least capable**. Their counterparts in **Saudi Arabia, the UAE, and China are rated positively** by their populace.

The financial impact sees countries experiencing varying degrees of financial loss due to scams. The highest average amounts stolen affect **Singaporeans ($4,031), the Swiss ($3,767), and Austrians ($3,484)**. The vast amounts stolen have resulted in severe financial repercussions worldwide, totaling a staggering **$1.026 trillion in losses, or 1.05% of the global GDP**.

Worst hit by fraudsters, **Kenya lost nearly 4.5% of its GDP to scams**, followed by **Vietnam (3.6%), Brazil & Thailand (3.2%)**. On the other end of the scale, **Belgium (0.11%), Ireland (0.12%), and the Netherlands (0.18%) lost the least**. The rate of recovery is low, since **only a fraction (7%) successfully recovered their lost funds**.

Beyond financial loss, the worldwide emotional toll stands significant, with **59% of scam victims reporting a substantial emotional impact**, underscoring the global ramifications of scams against general wellbeing, transcending geographical boundaries.

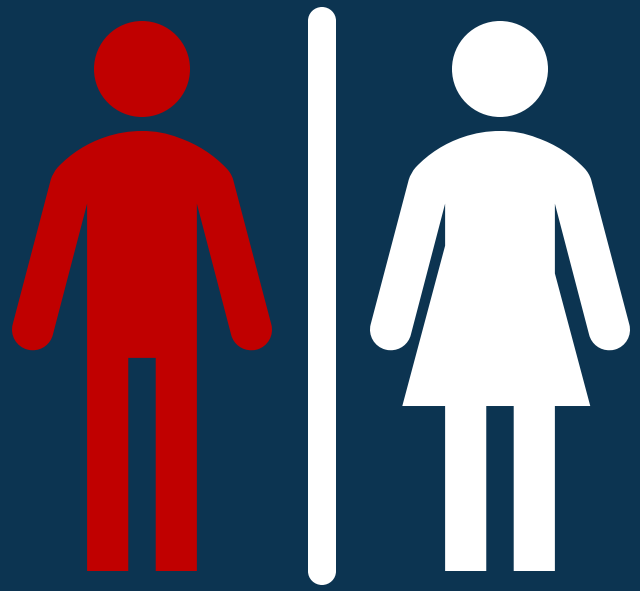
The 2023 Global State of Scams report serve to highlight the pervasive threat of scams, which transcend geographical boundaries and destroy lives worldwide. We hope that while digesting this huge amount of information, you will consider joining us to **turn the tide on scams**.

Best regards,

General Manager
ScamAdviser & Global Anti Scam Alliance

49,459 people from 43 countries participated in the Global State of Scams survey

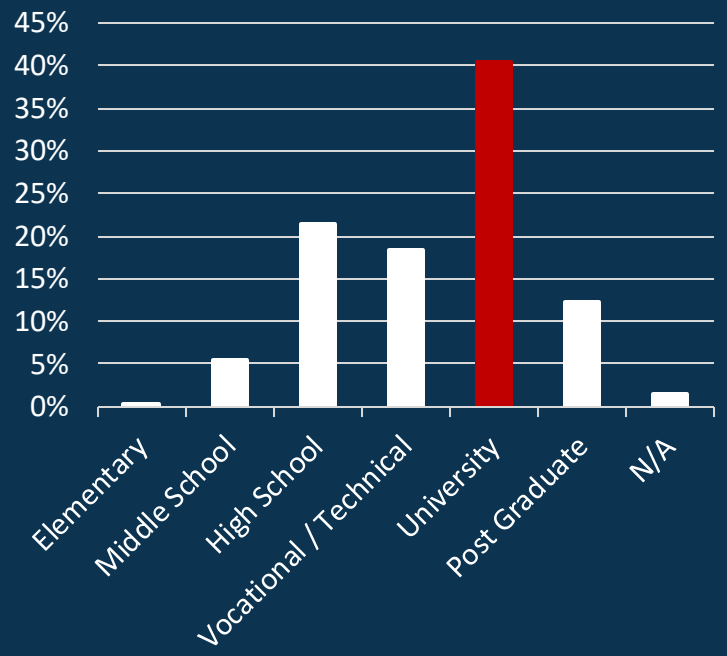
Gender



53% 47%

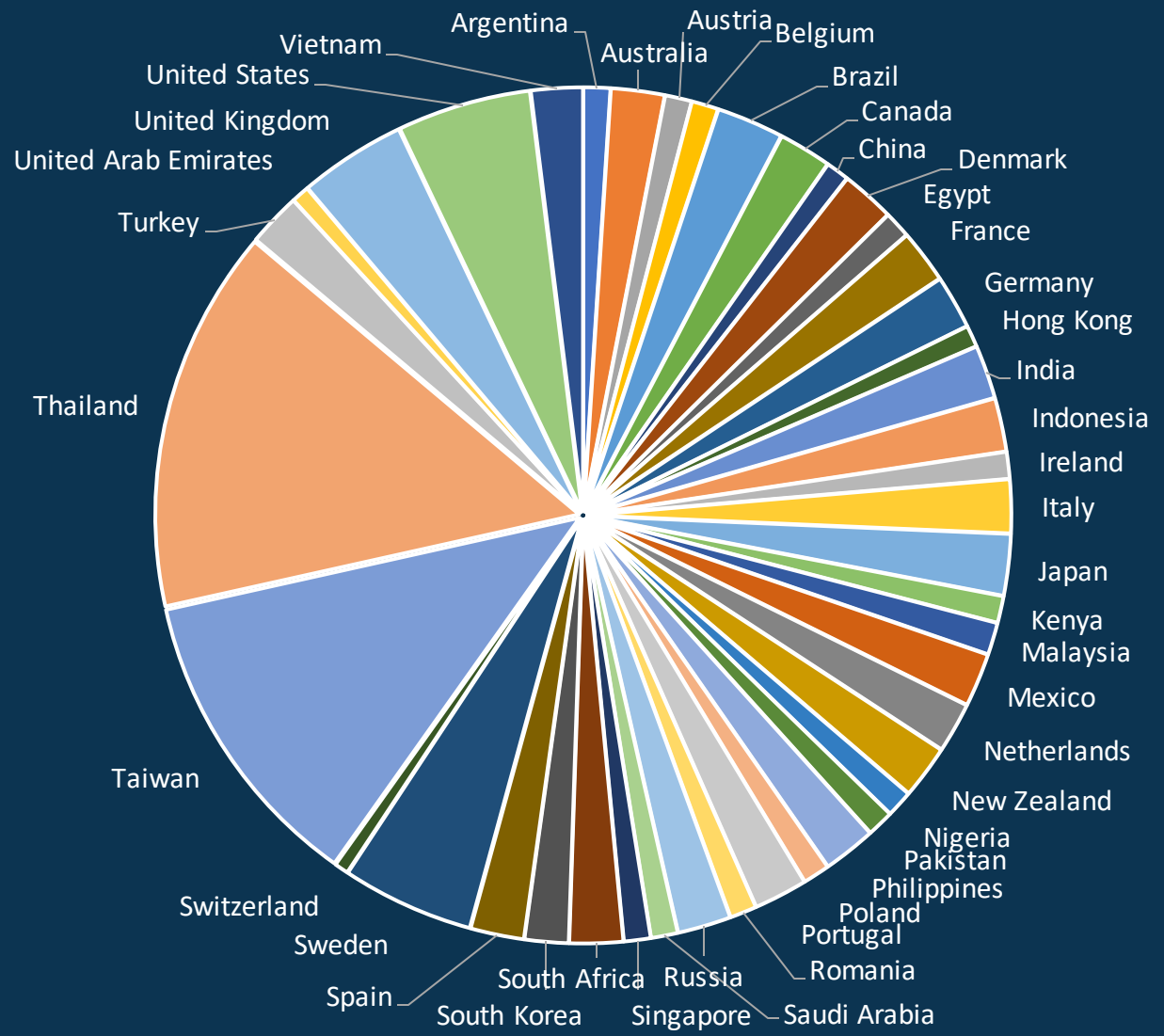
Age

Education



Especially in developing countries, more men than women participated, falling primarily into the 35–44 age group with a university degree.

The aggregated results have been normalized for country population



Per country, we strived for at least 500 respondents using Pollfish and national partners* to gather participants.

* Our national partners in Nigeria were able to supply the responses of 498 persons; United Arab Emirates, 350; China, 433; Hong Kong, 402; Switzerland (German-speaking), 260.

Taiwan's Fight Against Scams: A Chat with Jeff Kuo, CEO of Gogolook

In the digital age, scams and misinformation have emerged as persistent threats to individual and societal security. In Taiwan, a country at the forefront of technology adoption, these threats have manifested in various forms, including investment fraud and online shopping scams. We sat down with **Jeff Kuo, CEO of Gogolook and Director of Asia at GASA**, to discuss the current state of scams in Taiwan and the steps being taken to counter them.

How big have scams become in Taiwan? The issue of scams in Taiwan is indeed sizable and has been escalating for the past two decades. Apart from the traditional financial scams that most people are aware of, misinformation is becoming a major concern. This can often be orchestrated to mislead the populace, with geopolitical issues being a prime topic in Taiwan. According to the Gogolook Annual Fraud Report, scams and rumors have been spreading rampantly through messaging apps. For instance, Gogolook's AI-powered fact-checking chatbot, Auntie Meiyu, verified or debunked suspicious information 1.67 million times in 2022 alone. Scammers utilized the pandemic to proliferate misinformation & fraud, with a notable shift towards instant messaging apps and online forms, to steal personal information. The same report noted over 2,000 fraudulent domains created monthly, with nearly 60% related to investment scams. These findings underscore that the Taiwanese are entrenched in a cyberwar, where misinformation and scams are rampant, targeting individuals eager to adapt to new technology trends without fully assessing the associated risks.

Which scams stood out the last year in your Taiwan? The last year witnessed a significant rise in investment frauds, primarily through social channels, as highlighted in Gogolook's Annual Fraud Report. In addition, online shopping scams are trending, where consumers are often enticed by the allure of low prices or trendy items, only to never receive the items or have their financial details compromised. While impersonation scams via calls are an issue, growth has been slower compared to the spike in online shopping & investment scams.

Which actions have been taken by your government and other organizations to protect consumers from scams? Any best practices from which we can learn? The Taiwanese government has initiated measures to curb scams. The president issued executive orders that compel media channels to disclose advertiser details if they run scam ads, with non-compliance attracting fines. Various governmental agencies have implemented strategies to fight scams, such as *The Executive Yuan* launching the Anti-Fraud Office & proposed amendments to existing laws to impose heavier penalties for deep fake frauds. The *Ministry of Digital Affairs (MODA)* working to establish a defense platform for sharing cyber threat information and promoting the use of cryptography to secure e-commerce logistics information. The *National Police Agency (NPA)* established an Anti-fraud Hotline to crack down on fraudulent calls & promote private AI tools like Whoscall. The *Financial Supervisory Commission (FSC)* instructed online platform operators to remove fraudulent ads to curb online fraud & regulate account opening applications for reported warning accounts.

Which actions have been taken by your government and other organizations to protect consumers from scams? To truly empower consumers, fostering a community-centric approach where everyone collaborates is vital. This would mean public and private sectors joining hands to share relevant data to equip individuals with the information needed to counter frauds. At Gogolook, we believe in this collaborative model and continually seek partnerships with governments & NPOs to help consumers shield themselves from scammers.

Through collaboration and the utilization of technology, there's hope to turn the tide against scammers and protect the Taiwanese community at large.

Jeff Kuo
CEO, Gogolook
&
Director Asia, GASA

Gogolook GASA
Global Anti-Scam Alliance

Unveiling the Cybercrime Landscape: An Interview with L. Wes Quigley of the FBI IC3

In recent Internet Crime Report by the FBI's Internet Crime Complaint Center (IC3), the figures show an alarming increase in financial losses due to cybercrime, despite a decrease in the number of complaints. To understand these contrasting trends and delve deeper into the cybercrime landscape, we sit down with **L. Wes Quigley**, who speaks on behalf of the **FBI IC3 unit**. He provides insights into the findings of the report, the evolving threats, and the proactive measures taken by the IC3 to combat these digital dangers.

Mr. Quigley, the last FBI IC3 Internet Crime Report reveals a staggering number of complaints amounting to 800,944, with losses exceeding $10.3 billion. Despite a decrease in complaints by 5%, dollar losses have risen significantly by 49%. How does the FBI IC3 explain these contrasting trends? The contrasting trends can be attributed to the evolving nature of cybercrimes. While there's a decrease in the number of complaints, cyber actors are deploying more sophisticated and high-impact tactics that are leading to higher financial losses. Scams related to investments and cryptocurrencies are examples, where fewer incidents can lead to substantial losses.

Phishing schemes have been identified as the number one crime type with 300,497 complaints. However, the associated dollar loss of $52 million is comparatively small to the $3.3 billion loss from investment fraud. Why is there such a discrepancy, and how is the FBI addressing this? Phishing schemes tend to involve smaller amounts of money per incident, or no loss, but occur at a high frequency. On the other hand, investment fraud often involves larger sums, resulting in a higher total financial loss despite fewer occurrences. The FBI is committed to addressing both by educating the public about the various types of scams and working with law enforcement and private sector partners to investigate and mitigate these threats.

Investment fraud related to cryptocurrency has seen a massive increase, from $907 million in 2021 to $2.57 billion in 2022. How is the FBI adapting to this emerging threat, especially given the anonymity associated with cryptocurrencies? The FBI is continuously adapting its strategies to emerging threats, including cryptocurrency-related fraud. We're working closely with experts in cryptocurrency and blockchain technology to enhance investigative capabilities. Additionally, we are focused on public awareness campaigns to inform people about the risks involved with cryptocurrency investments and provide guidance on how to invest safely.

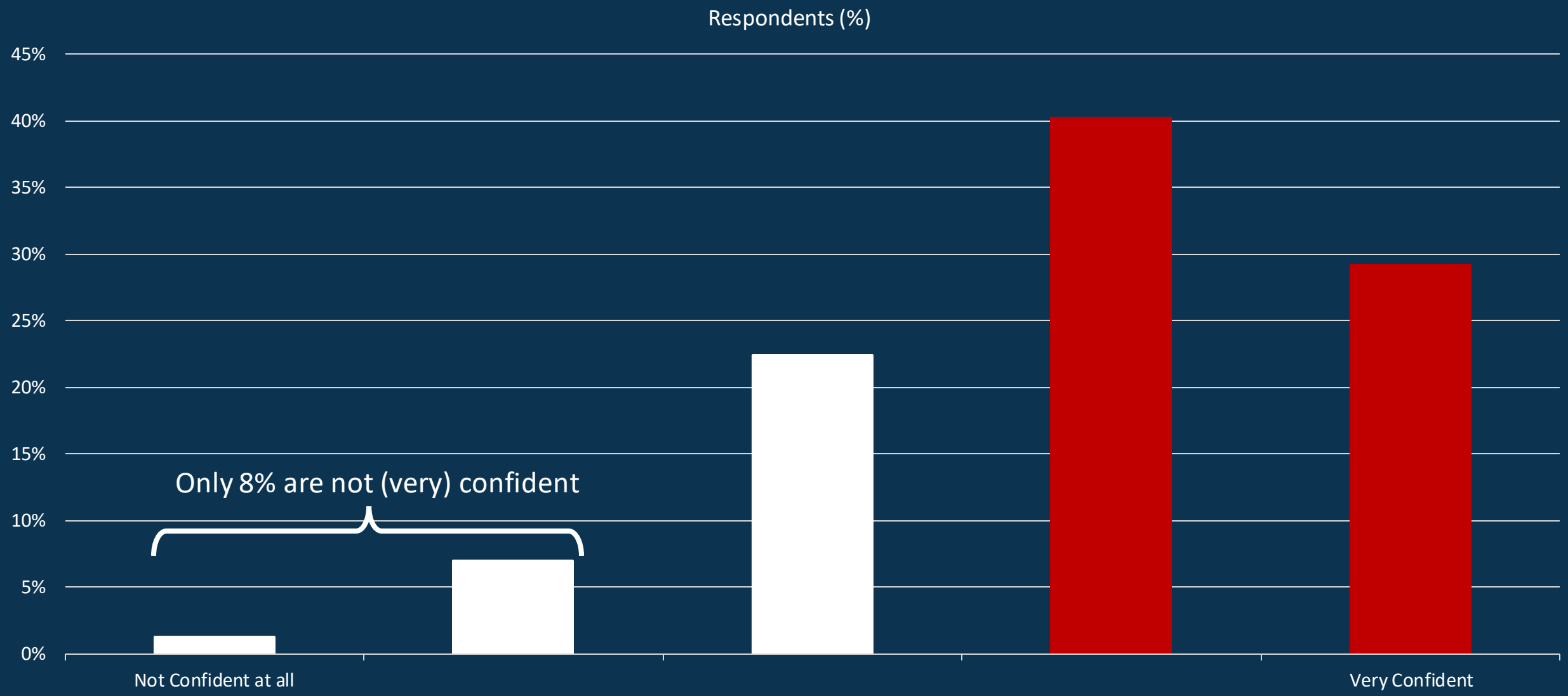
Can you expand on the work that FBI is doing in partnership with law enforcement and private sector partners to tackle cybercrimes? Certainly! The FBI is fostering collaborations with various law enforcement agencies and private sector entities. By sharing information and insights, we can stay ahead of cybercriminal trends and develop more effective strategies for preventing cybercrimes and assisting victims. Our partnerships are crucial for advancing investigations and holding cybercriminals accountable, irrespective of their location.

Lastly, considering the escalating cyber threats, what is the FBI's message to the public, and how can they protect themselves better against these threats? The FBI urges the public to remain vigilant and informed about the various types of cybercrimes and the methods cybercriminals use. We encourage everyone to review consumer and industry alerts published by IC3 regularly. Employing good cyber hygiene practices, such as using strong, unique passwords and enabling two-factor authentication, can provide significant protection. If victimized, it's crucial to report the incident to IC3 and your local FBI field office, as this information is invaluable in tracking, investigating, and mitigating cybercrimes.

The IC3's unwavering commitment to facing these cyber threats head-on, by working closely with law enforcement, private sector partners, and the public, provides a beacon of hope and reassurance in these technologically turbulent times.

L. Wes Quigley
UC, Internet Crime Complaint Center (IC3),
Federal Bureau of Investigation (FBI)

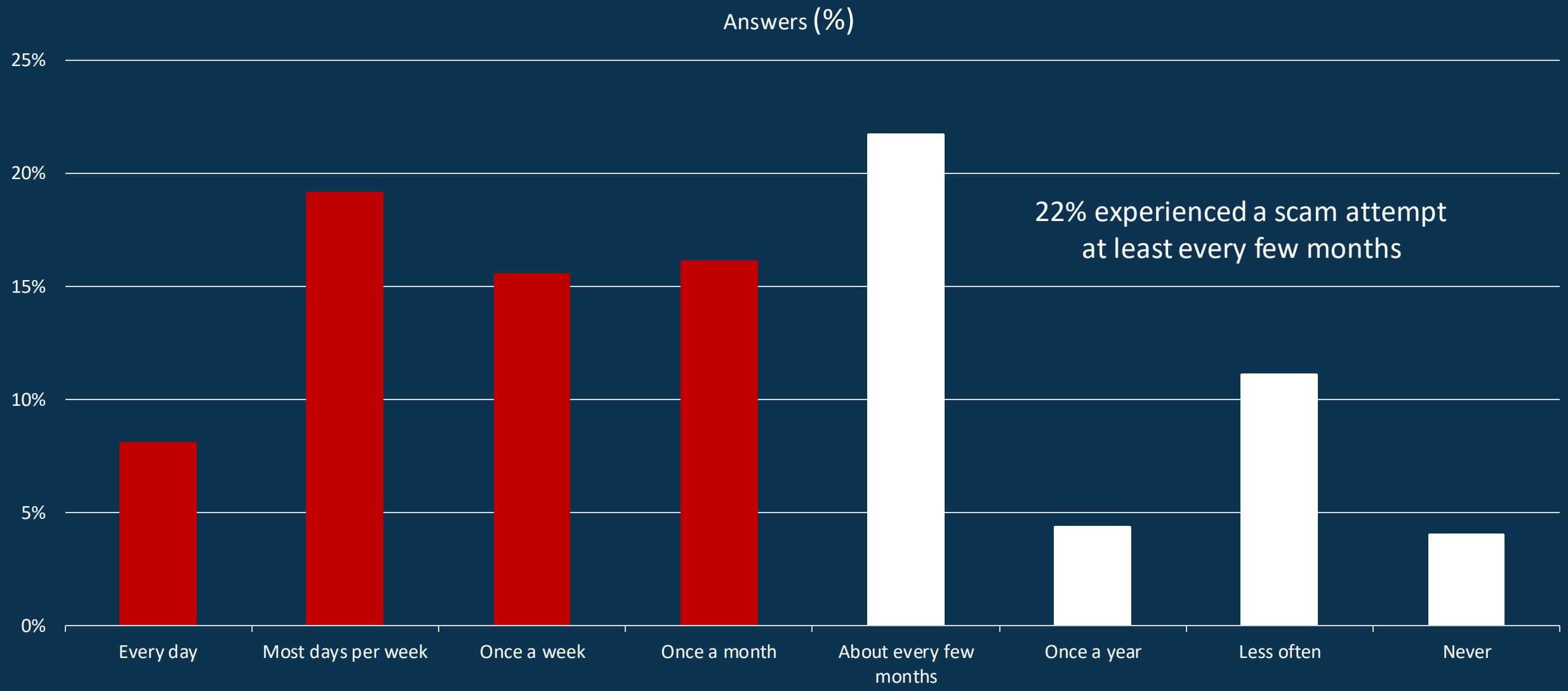
69% of the participants are (very) confident that they can recognize scams



Indonesia (84%), Egypt (76%), Nigeria & Kenya (74%) and India (72%) are the most confident.
Japan (32%), Malaysia (43%), South Korea (45%), France (46%) are the least confident.

Q2: How confident are you that you can recognize scams and deceit?

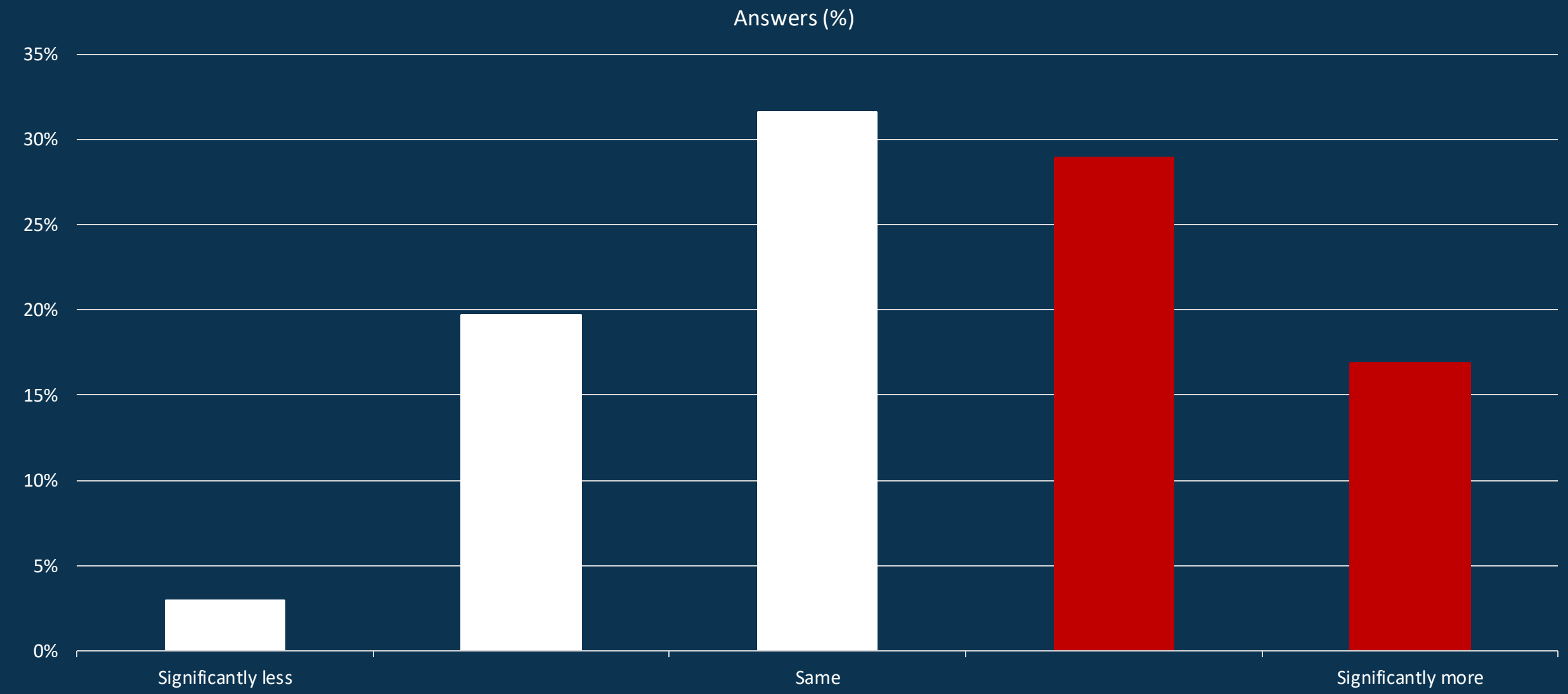
59% of the participants encounter a scam at least once per month



Citizens from Hong Kong (90%), Brazil (81%), Malaysia (79%), Thailand (78%), Australia & Canada (76%) are approached the most Polish & Saudi (40%), Romanians (47%), Dutch (48%) and Austrians (49%) are approached the "least."

Q3: In the last 12 months, how frequently have you encountered scams including deceptive advertising, phishing/fake emails/texts, phone calls, etcetera)?

45% of the surveyed people experienced more scams in the last 12 months



Globally, only 3% experienced fewer scams than the previous year. Hong Kong experienced the strongest growth (71%), followed by Singapore (63%), Australia, Nigeria, and Kenya (61%).

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

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.

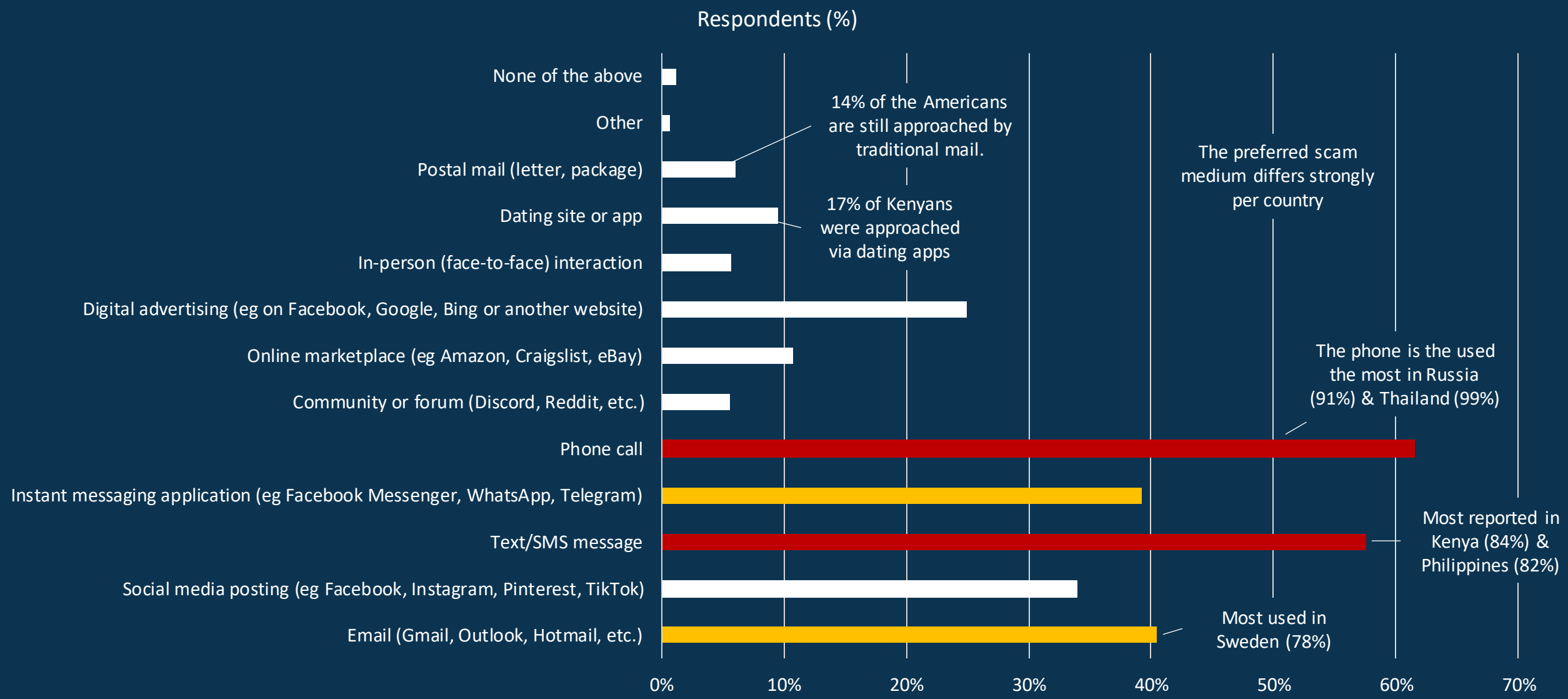
What action is needed now to give consumers the upper hand in the fight against scams? The coordination of regulatory actions is critical. Alongside the Online Safety Bill, the UK Government is working on the Online Advertising Programme to regulate advertisements hosted on websites outside the scope 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

Fighting Economic Crime Together

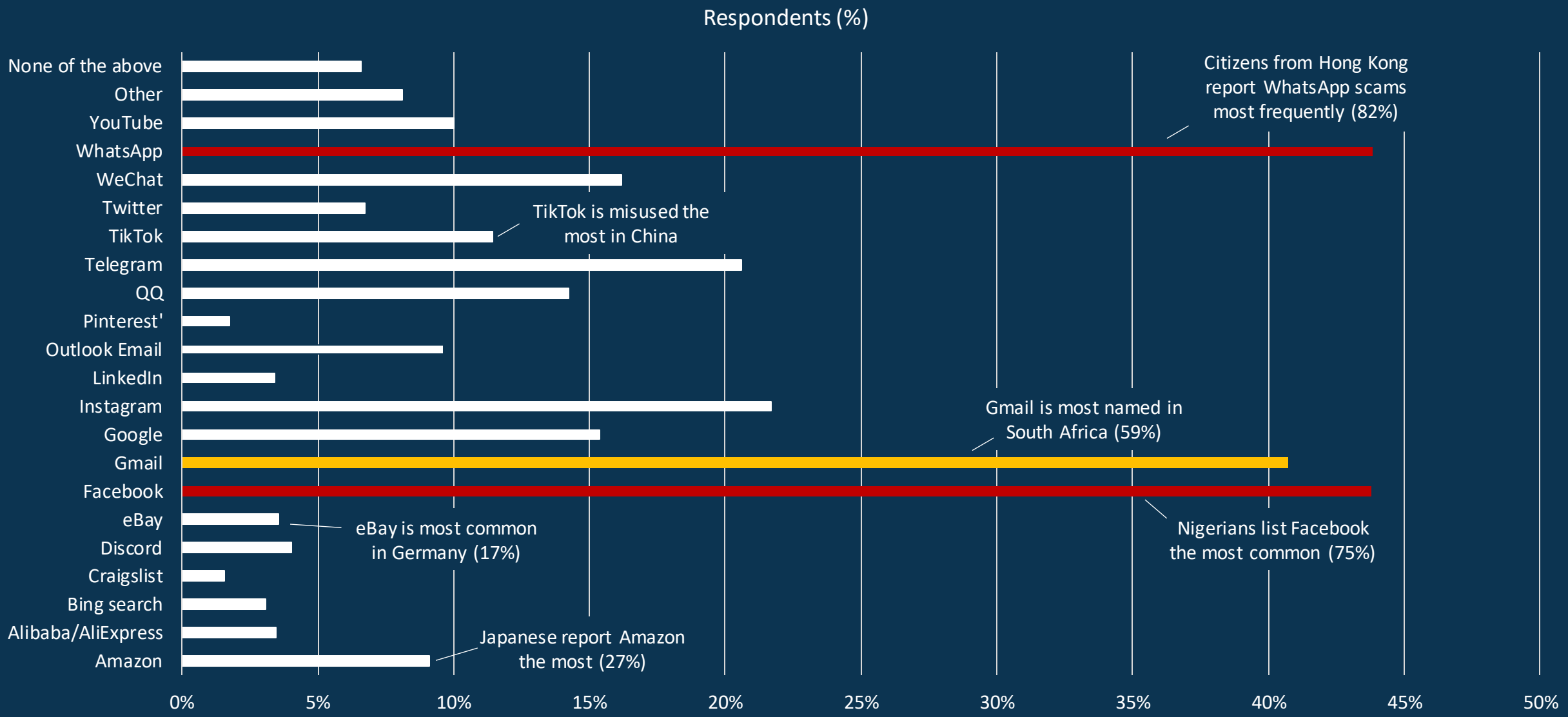
Phone (61%) and Text/SMS messages (58%) are the most common scam media



Followed by Email (40%) and instant messaging apps (39%).
Traditional mail and face-to-face scams are the least common methods of scamming people (each 6%).

Q5: Through which communication channel(s) did scammers mostly try to approached you in the last 12 months? Choose up to 3.

Facebook and WhatsApp (both named 44%) are the platforms most used by scammers



The third place is taken by Gmail (41%). Local players are also named such as Yahoo!, Shopee, LINE & Mercari.

Q6: Via which platform(s) did scammers mostly try to contact you in the last 12 months? Choose up to 3.

Guardians of Trust: Amazon's Proactive Frontline Against Impersonation Scams

In a world grappling with an escalating tide of impersonation scams, global businesses must bring initiatives to curb fraudulent activities and shield consumers. **Abigail Bishop**, **Head of External Relations, Scam Prevention at Amazon** delves into the intricacies of the ongoing battle against impersonation scams, emphasizing the need for strategic, collective efforts to foster a safer digital environment.

How big have impersonation scams become? Scams are an industry-wide issue that misuse multiple trusted entities, including financial institutions, communications providers, and other trusted brands. It is difficult to understand the full scale of the challenge with multiple entities seeing only a piece of the scam and the continued challenge of victim underreporting. Third-party consumer groups and government agencies provide valuable aggregated information about the broader landscape of impersonation scams. Data released by the Federal Bureau of Investigation's Internet Crime Complaint Center reported that losses exceeded $10.3 billion in 2022.

Which impersonation scams stood out in 2023? In 2023, the complexity of scams escalated with individuals often being targeted through social media, fake tech support calls, or fraudulent transaction confirmations. The most reported impersonation scam to Amazon was fake "suspicious activity" alerts, constituting over a quarter of all reports. Scammers tricked customers into believing their Amazon account was compromised, prompting them to click on fraudulent links or share personal details to "verify" their accounts, potentially leading to stolen payment or login information. To combat this, we collaborated with the Global Anti-Scam Alliance to provide consumers with guidance to recognize and avoid this prevalent scam tactic.

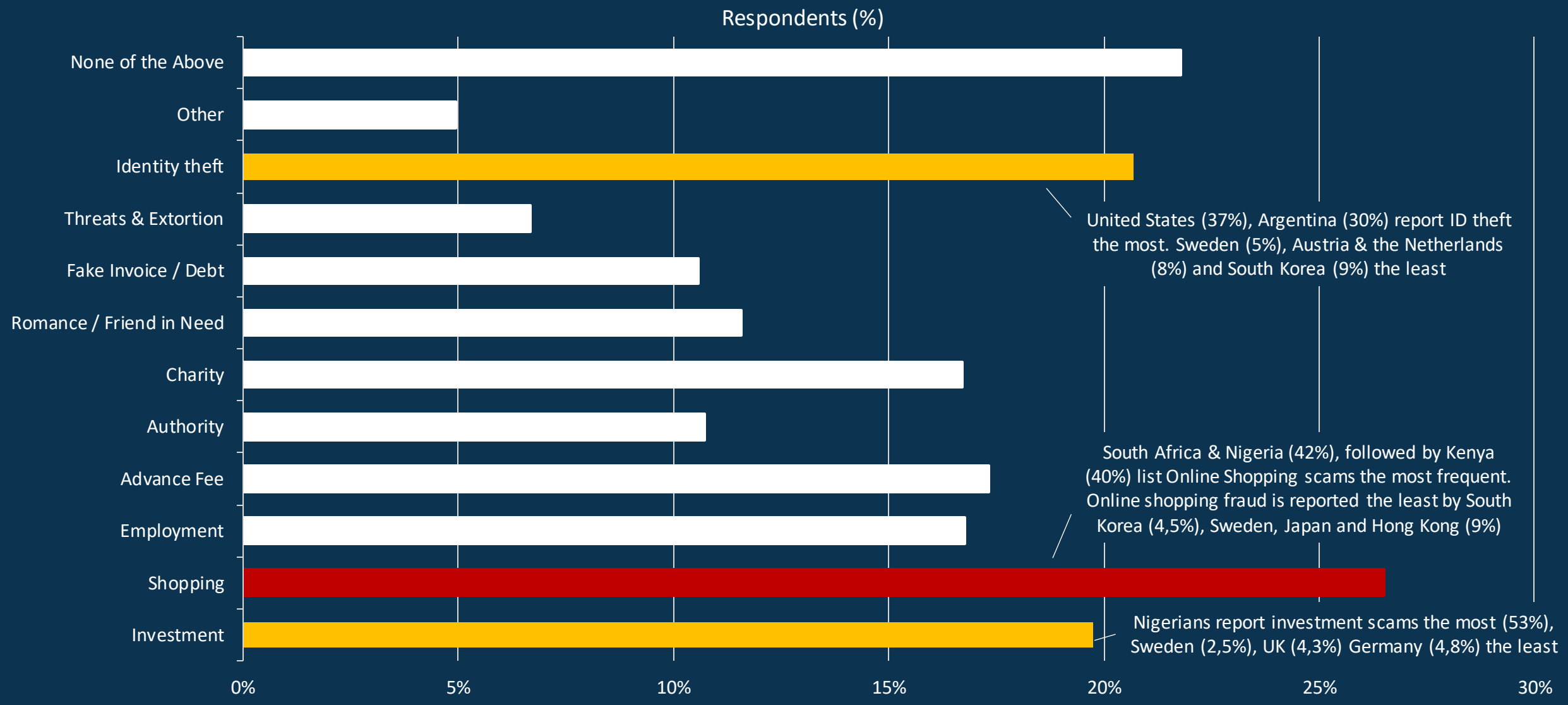
Which actions have you been taken to protect consumers from impersonation scams? We have zero tolerance for criminals who pretend to be Amazon to commit fraud. Our obsession with customers motivates our commitment to ensure scammers are not using our brand, or anyone else's, to take advantage of people who trust us. We protect consumers from scams by educating, innovating, and holding bad actors accountable. In 2022, Amazon initiated takedowns of more than 20,000 phishing websites, 10,000 phone numbers being used as part of impersonation scams and referred hundreds of bad actors globally to local law enforcement authorities. We also make it harder for bad actors to copy our communication by employing industry-leading practices. Our recent broad adoption of email verification technology, across more than 20 countries, makes it easier for consumers to distinguish authentic communications from Amazon. This is just one of many solutions that we have implemented to protect consumers.

What action would you like to see taken in the future that could give consumers the upper hand in the fight against scams? Our vision is to build a world where consumers are confident that they will not be taken advantage of by bad actors who impersonate trusted brands. While Amazon will remain vigilant and persistent in our efforts to stay one step ahead of fraudsters, impersonation scams are an industry-wide issue, and we cannot win this fight alone. When it comes to protecting against scams, knowledge is power, and we are reaching beyond our customer base to empower consumers through education. As part of this, we partner with leading organizations to educate consumers on how to avoid falling victim to scams. We also issue and promote resources and tips to help consumers identify scams. For example, our **Cybersecurity Awareness Training** is free and available to everyone.

By fostering partnerships and extending educational resources beyond their customer base, Amazon is working to realize a future where scammers are put out of business. As they strive to remain a step ahead of the fraudsters, their efforts resonate with a powerful message: that in the battle against scams, knowledge isn't just power; it's the shield that safeguards the trust and security of consumers worldwide.

Abigail Bishop
Head of External Relations
Scam Prevention
Amazon

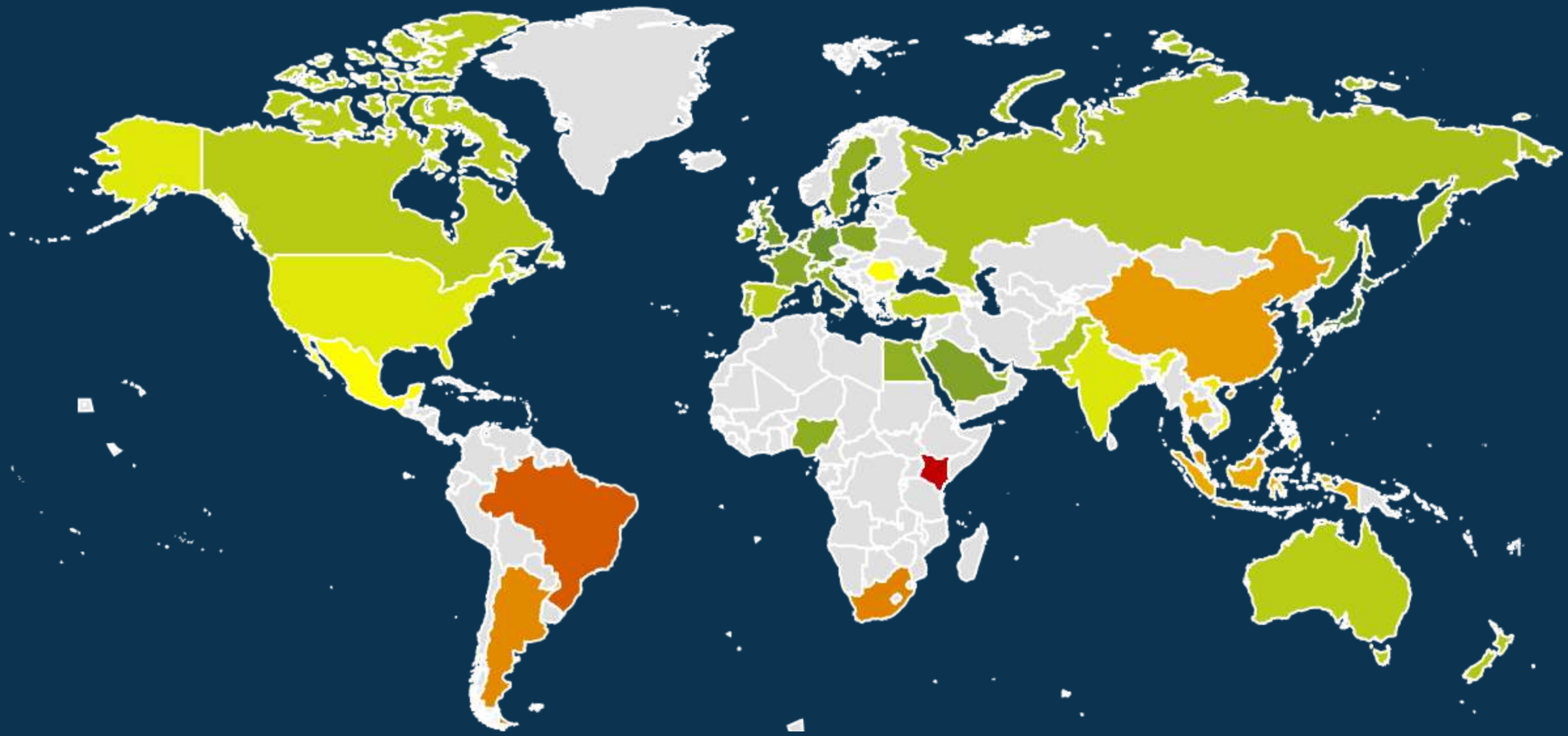
Globally, 78% participants experienced at least one scam in the last 12 months



Shopping Scams are occurring the most (27%), followed by Identity Theft (21%) and investment fraud (20%).

Q7: Which of the following situations happened to you in the last 12 months? Select all that apply.

Kenyans (49%), Brazilians (41%), and South Africans (38%) lost money most often



Other countries with frequent capital loss are Argentina (37%), Malaysia (36%), China (35%), and Indonesia (34%).
Japan (4%), Austria & Germany (8%), Belgium & Netherlands (9%) report the least instances of money lost in the last 12 months.

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".

Brazil Targets Online Fraud Increase with New Tactical Plans & Severe Penalties

Brazil, a country renowned for its vibrant culture and picturesque landscapes, has not escaped the escalating trend of scams, especially in the digital domain. Despite its rapid technological advancement and embracement of digital platforms, it finds itself grappling with a significant increase in scams, leveraging the new technologies that have pervaded every aspect of daily life. We spoke with **Rafael Fernandes, Prosecutor & Chief Planning Officer at the Prosecution Office of the State of Minas Gerais (MPMG)**, to gain insights into the current scenario of scams in Brazil and the countermeasures being adopted.

Can you paint a picture of the current scam situation in Brazil? Absolutely, scams have soared in Brazil recently, with several studies highlighting the nation as one with a high incidence of scams. Norton revealed that almost a third of the population, roughly 71 million people, were targeted last year. Furthermore, a survey by Brazil's national federation of banks, Febraban, indicated that the victims of financial scams have increased from one in five to nearly one in three Brazilians within a span of a year. The surge in online scams, particularly after the onset of the pandemic & the launch of the PIX payment system, has been substantial. Kaspersky noted a striking increase in phishing attempts to over 134 million between July 2022 and July 2023, placing Brazil first in Latin America and sixth globally in phishing attacks. Alarmingly, a considerable discrepancy exists between the actual number of scams and the reported cases, with at least 585,946 online scams reported to authorities, highlighting a critical area for improvement in reporting and tracking.

Which scams have surged in popularity in the last year in Brazil? Absolutely, last year we saw a significant prevalence of scams involving WhatsApp cloning, bank fraud, fake bank slips with altered barcodes, PIX scams, and investment scams among others. Instagram scams and fake loan scams also had a notable presence, albeit lesser compared to the peak in 2021.

What steps have the government & other organizations undertaken to shield consumers from scams? In 2021, Brazil bolstered its legal framework against scams, introducing a new 'online fraud' crime category with 4 to 8-year penalties. Additionally, specialized units formed at state prosecution offices to combat cybercrimes. In 2022, the Federal Government launched a Tactical Plan to Combat Cyber Crimes, enhancing inter-agency collaboration and information sharing. Notable partnerships between the Federal Police & Febraban, and awareness campaigns "Pare e Pensa" & "Chegando Junto," educate the public & foster preventive actions against scams.

What further initiatives do you propose to empower consumers in their fight against scams? Addressing the complexity of scams requires a multifaceted approach, involving not just the government but also tech giants and society at large. Firstly, a legal framework demanding greater responsibility from Big Tech in policing fraudulent content on their platforms would be beneficial. Secondly, fostering dialogue & cooperation between the public sector, the justice sector, and the society is essential. Further, it would be prudent to facilitate collaborations between tech giants & government agencies to counter scams effectively. Lastly, significant investments in Civil Police & the Public Prosecutor's Office for training and creating specialized units equipped with appropriate technological tools can significantly enhance our capabilities in investigating and prosecuting cybercrimes, including online scams.

With continuous efforts from the government & collaborating private entities, Brazil will strengthen its digital infrastructure, fostering a safe & secure online environment for its citizens. The insights from Rafael Fernandes underscore the commitment to adapt & forge ahead, ensuring the safety and wellbeing of Brazilians.

Rafael Fernandes
Prosecutor & Chief Planning Officer
Prosecution Office of the State of Minas Gerais

MPMG
Ministério Público
do Estado de Minas Gerais

SAFPS Warns Advanced Fee & Investment Scams are Proliferating in South Africa

South Africa, despite its economic potential and growing tech-savvy population, is grappling with a dramatic surge in scams and cybercrimes. The **Southern African Fraud Prevention Service (SAFPS)**, represented in the Global State of Scams report by **Nazia Karrim**, stands as a bulwark against these threats, fostering cross-sector collaboration to combat fraud and safeguard consumers. SAFPS services include access to fraud databases, identity verification via the Dep. of Home Affairs, biometric verification, and data analysis. Providing access to vital fraud prevention tools to consumers and 50+ corporate members. SAFPS members access to Fraud, Scam & Victim listings, Protective Registrations, and Financial Crime Analytics.

Just how prevalent have scams become in South Africa lately? The volume of scam incidents has surged remarkably in recent years. The DPCI, a division of the South African Police Services, has even set up a dedicated task team to address this. Based on fraud incidents reported to SAFPS over the past five years, we've observed a 600% increase in 2022 compared to 2018. More startling is the 150% increase in scam volumes reported by our members in 2023 compared to the previous year.

Were there any scams in the past year that really caught everyone's attention or seemed to be the latest "trend" in South Africa? Incident volumes reported to SAFPS via our Yima online reporting tools show that advanced fee scams and investment scams have been most prevalent, making up 33% and 24% of incident volumes, respectively. This is significant, especially since the Yima scam prevention and awareness program has only been functional for five months. Online scams, specifically those related to goods and services like vehicle purchase scams, have also been rampant. One of the emerging trends is Ancestry scams, which exploit African cultural beliefs. Victims are often duped by fraudsters pretending to be traditional healers. The losses are substantial, sometimes even involving the sexual abuse of female victims. Many such incidents go unreported due to fear. In terms of organized crime, the Black Axe syndicate was notably dismantled in 2022 in a joint international operation.

How are the government and other organizations stepping up to protect people from scams? Are there any standout strategies or collaborations? Both public and private sectors are collaborating, with support from Law Enforcement. Specialized task teams, like the DPCI 419-Scams Task Team, and the South African Cyber Fraud Task Team have been initiated to comprehensively tackle this issue, encompassing prevention, detection, and apprehension. Furthermore, specialized training and public awareness campaigns, spearheaded by SAFPS in partnership with the public and private sectors, are in place to educate citizens and stakeholders.

What more do you think can be done to empower consumers in this battle against scams? Law enforcement and corporate entities need to ramp up their roles in awareness and prevention. Investing in education, particularly at school and university levels, can instill a culture of active caution and preventative. Additionally, victims require support & clear direction when they realize they've been scammed. The legal system should encourage victims to come forward, enabling data collection that can lead to the identification of major fraud syndicates. It's concerning that only 20% of all incidents reported to SAFPS are relayed to the South African Police Services.

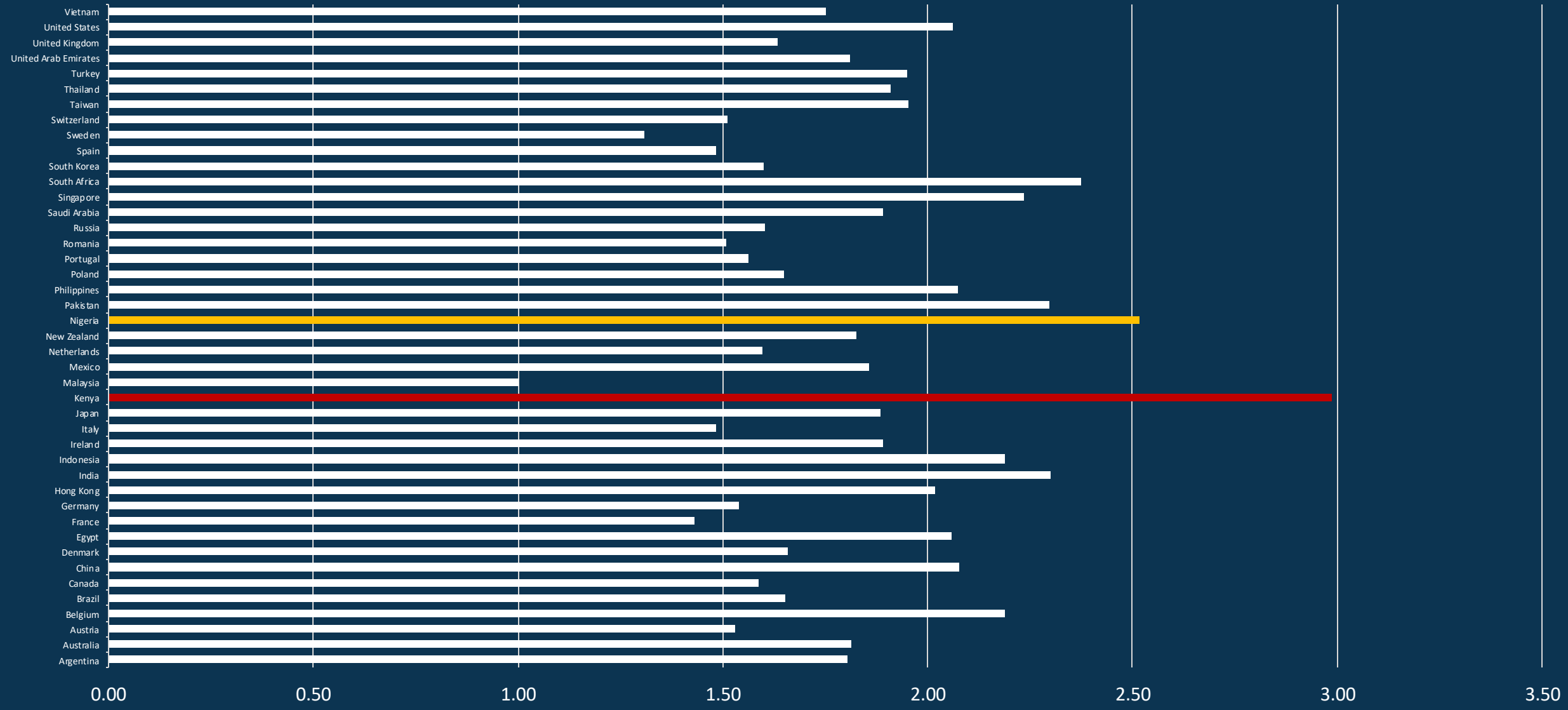
South Africa's journey in the digital age is a testament to both its potential and pitfalls. Insights from the Southern African Fraud Prevention Service illuminate the nation's dedication to confronting cyber threats, underscoring a united front and proactive initiatives to safeguard its citizens.

Nazia Karrim
Head of Product Development
Southern African Fraud Prevention Service (SAFPS)

SAFPS
SOUTHERN AFRICAN FRAUD PREVENTION SERVICE

YIMA
Stop. Think. Don't get scammed!
Tel: +27 (0)11 867 2234 info@yima.org.za www.yima.org.za
A product of the Southern African Fraud Prevention Service

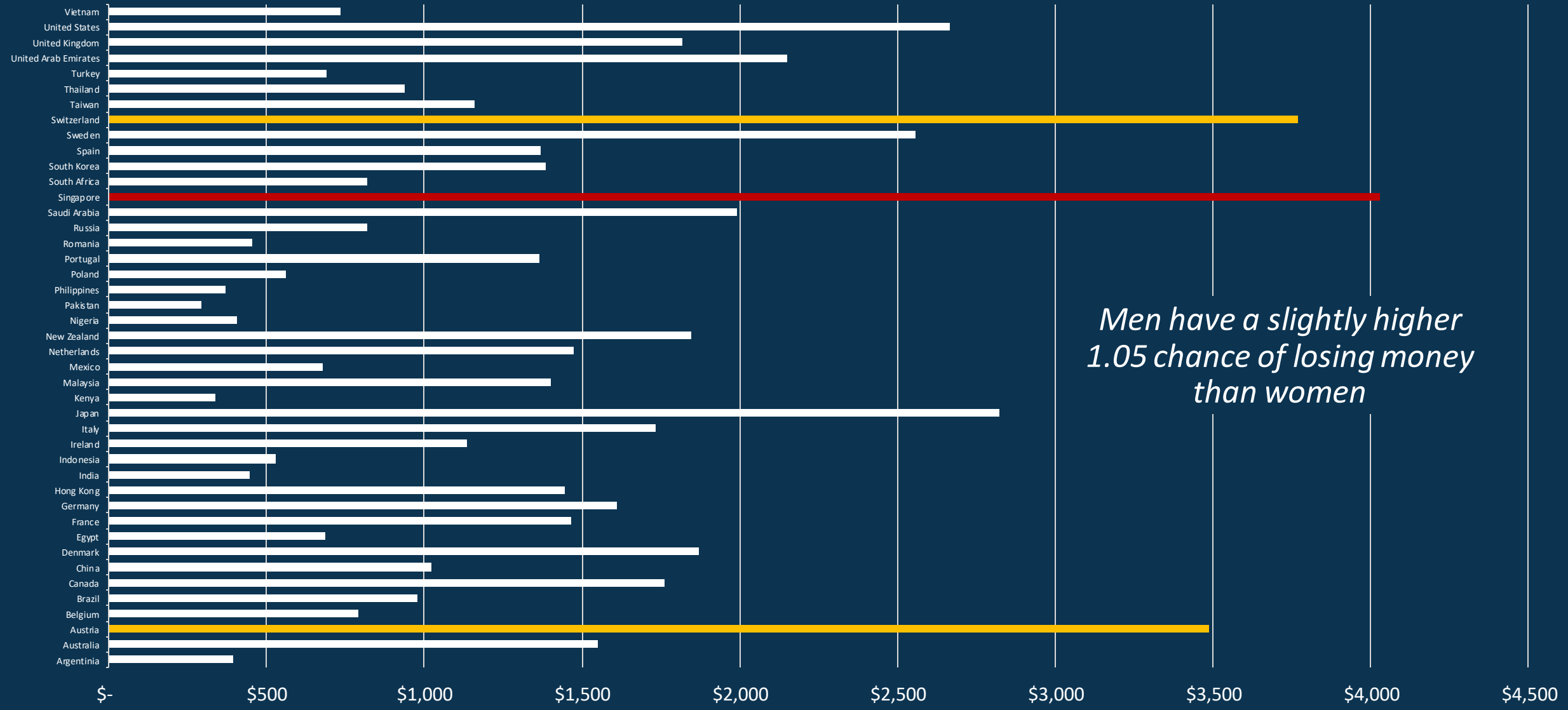
Revictimization is a huge issue: Kenyan victims get scammed almost 3 times each



Nigeria reports the 2nd highest revictimization rate of 2. In nearly all countries, the revictimization rate is above 1.5.

Q7: Which of the following situations happened to you in the last 12 months? Select all that apply.

The average amount lost varies drastically by country



The highest average amount stolen is in Singapore ($4,031) followed by Switzerland ($3,767) and Austria ($3,484)
The sheer number of investment scams has a significant impact on the average.

Q7: Which of the following situations happened to you in the last 12 months? Select all that apply.

Singapore's Ministry of Home Affairs Spearheads Bold Initiatives Against Rising Scams

Singapore, known as a haven of safety and security, hasn't been immune to the challenges of the digital era. Despite being recognized as the safest country globally in 2022, Singapore has witnessed a surge in online scams, which have become a principal factor driving the national crime rate. **Director of Policy Development & Security at the Ministry of Home Affairs Dr Ng** sheds light on this issue and the measures being taken to counteract it.

Singapore was named the safest country globally in 2022 by the Gallup Global Law and Order Report. However, the surge in scams challenges this status. How rampant have scams become in Singapore recently? Scams have grown at an alarming rate in Singapore. In contrast to our low and stable physical crime rates, scams have escalated over the past five years, with reported cases rising fivefold and losses quadrupling. Last year alone saw 31,728 cases reported, a 32.6% rise. Notably, platforms like WhatsApp, Telegram, Facebook and Instagram became hotspots for fraudulent activity, with phishing scams leading, followed by job and e-commerce scams.

What were the major scams in Singapore in 2022 and their impact? In 2022, Singapore saw a surge in phishing scams with 7,097 cases resulting in SGD 16.5 million in losses, closely followed by job scams with 6,492 cases and SGD 117.4 million lost. E-commerce scams persisted with 4,762 cases, accumulating SGD 21.3 million in losses, while investment scams led to SGD 198.3 million in losses from 3,108 cases. Fake friend call scams had 2,106 cases, causing SGD 8.8 million in losses.

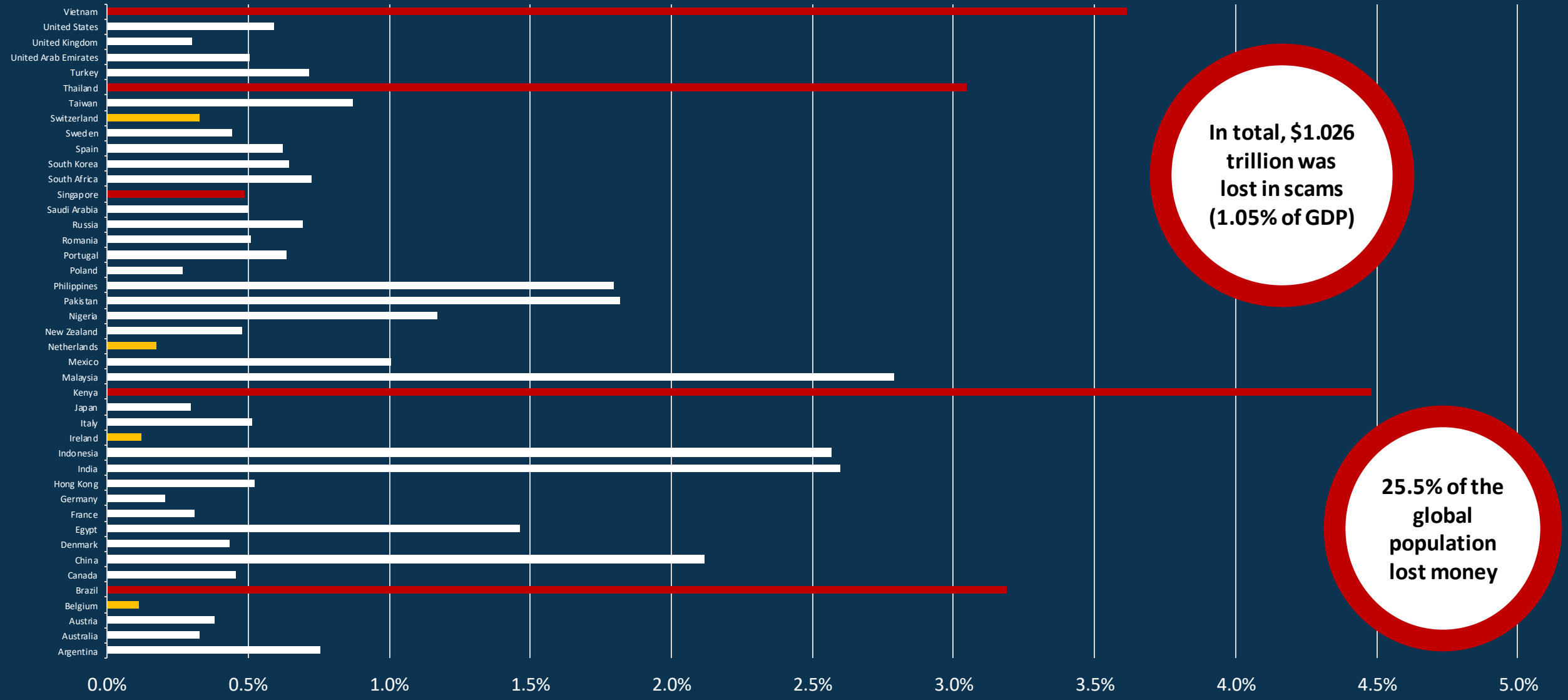
Could you share some of the steps Singapore has initiated to protect consumers from scams? To combat this menace, the Inter-Ministry Committee on Scams (IMCS) has spearheaded various strategies encompassing prevention, detection, enforcement, and education. The IMCS has initiated collaborative efforts with telecom companies and banks to secure communication infrastructure & banking channels, with measures like blocking spoofed numbers and requiring organisations to register their Sender IDs with the SMS Sender ID Registry (SSIR), to warn consumers about potential scam messages. The launch of the ScamShield mobile application facilitates easy reporting of scam calls & messages. A notable venture was the establishment of the Anti-Scam Command, co-locating police and banks to enhance coordination of anti-scam enforcement & investigations. On the education front, the national "I can ACT Against Scams" campaign launched in January 2023, guides individuals to Add, Check, and Tell - a three-step precautionary process to safeguard against scams.

Such comprehensive measures indeed make a difference. What further actions do you propose to give consumers an upper hand in the fight against scams? Firstly, enhancing our cross-border enforcement capabilities through international collaborations, such as establishing frameworks for swift asset recovery. This will facilitate quicker intervention, tracing the flow of scam proceeds and freezing fraudulent accounts promptly. Secondly, forging global norms for preventative measures against scams, including setting guidelines for online platforms to verify user identities and prevent the creation of inauthentic accounts. A re-calibration of the balance between security and user experience is essential, focusing on preemptive measures instead of post-scam enforcement.

In the face of growing challenges, Singapore, led by vigilant organizations like the Ministry of Home Affairs, continues to innovate and adapt, aiming to maintain its position as a safe and secure nation in the digital era.

Dr. Ng Li Sa
Director of Policy Development & Security, Policy Development Division, Ministry of Home Affairs, Singapore

Developing countries appear to lose a much higher percentage of GDP in scams



In total, $1.026 trillion was lost in scams (1.05% of GDP)

25.5% of the global population lost money

Kenya lost nearly 4.5% of its GDP to scams, followed by Vietnam (3.6%), Brazil & Thailand (3.2%). Belgium (0.11%), Ireland (0.12%) and The Netherlands (0.18%) lost the least.

Q7: Which of the following situations happened to you in the last 12 months? Select all that apply.

Scams are hurting consumers worldwide in many ways

“I was very shocked to see my credit card information compromised when I saw a charge to an unknown recipient. Turns out it is part of a Bank Identification Number (BIN) attack.”

“I bought a new pair of hunting boots that I never received or heard from them after initial confirmation email.”

"They (scammers) claimed to be in the military, and they, along with their comrades, needed help obtaining their bonuses. The gentleman professed love for me, and I ended up sharing all my personal info."

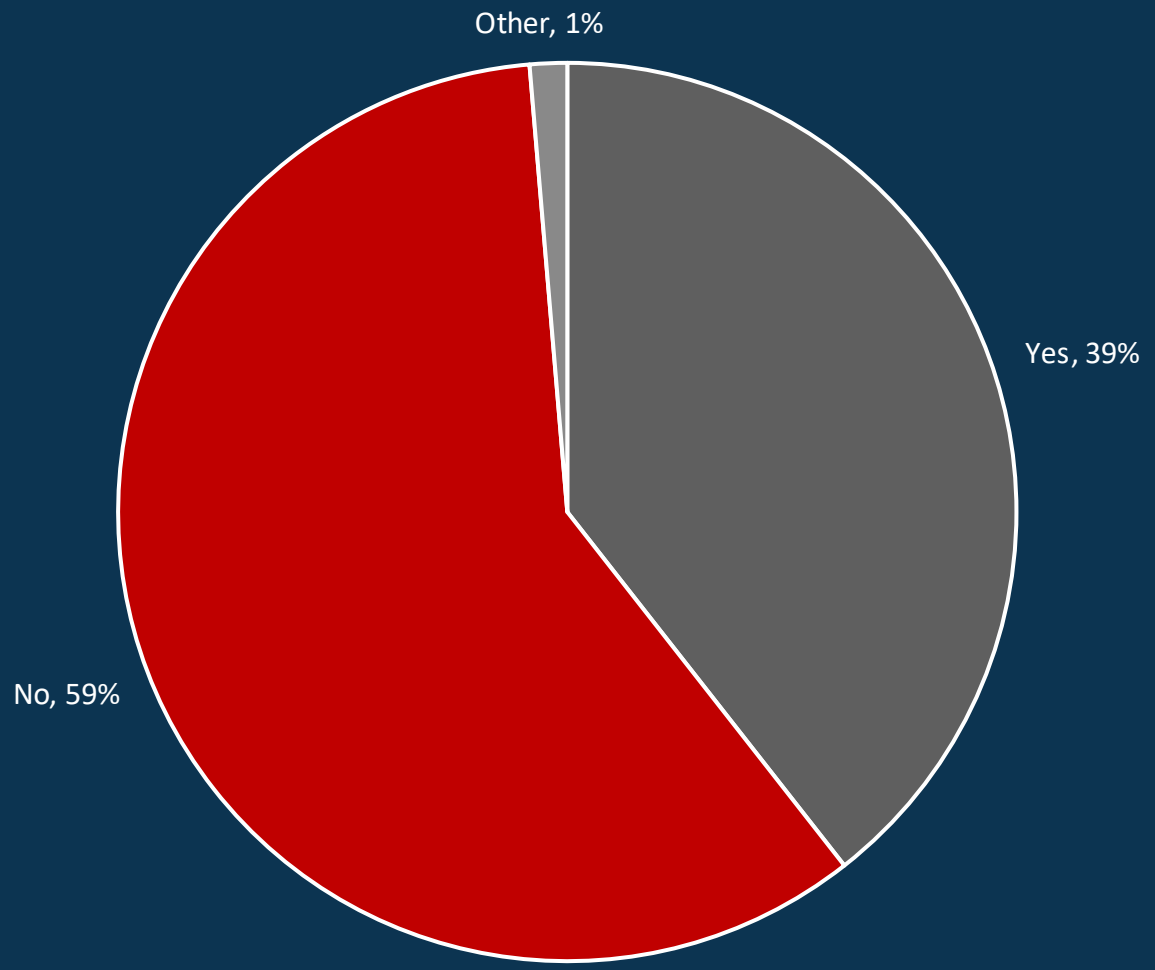
“He (scammer) claimed to be in the USA, sent valuable items, and asked me to pay for customs fees. I paid the invoice, only to realize later that it was a scam.”

“I came across an enticing online ad for an investment company promising substantial returns and quick payouts. The website had numerous positive, but fake, reviews. After I invested, there was no communication, but I noticed my money growing on their website. Eventually, they called, demanding more money for me to withdraw my funds.”

Q9: Regarding the negative experience that impacted you the most, describe what happened.

Globally, 59% did not report the scam to the police or other government authorities

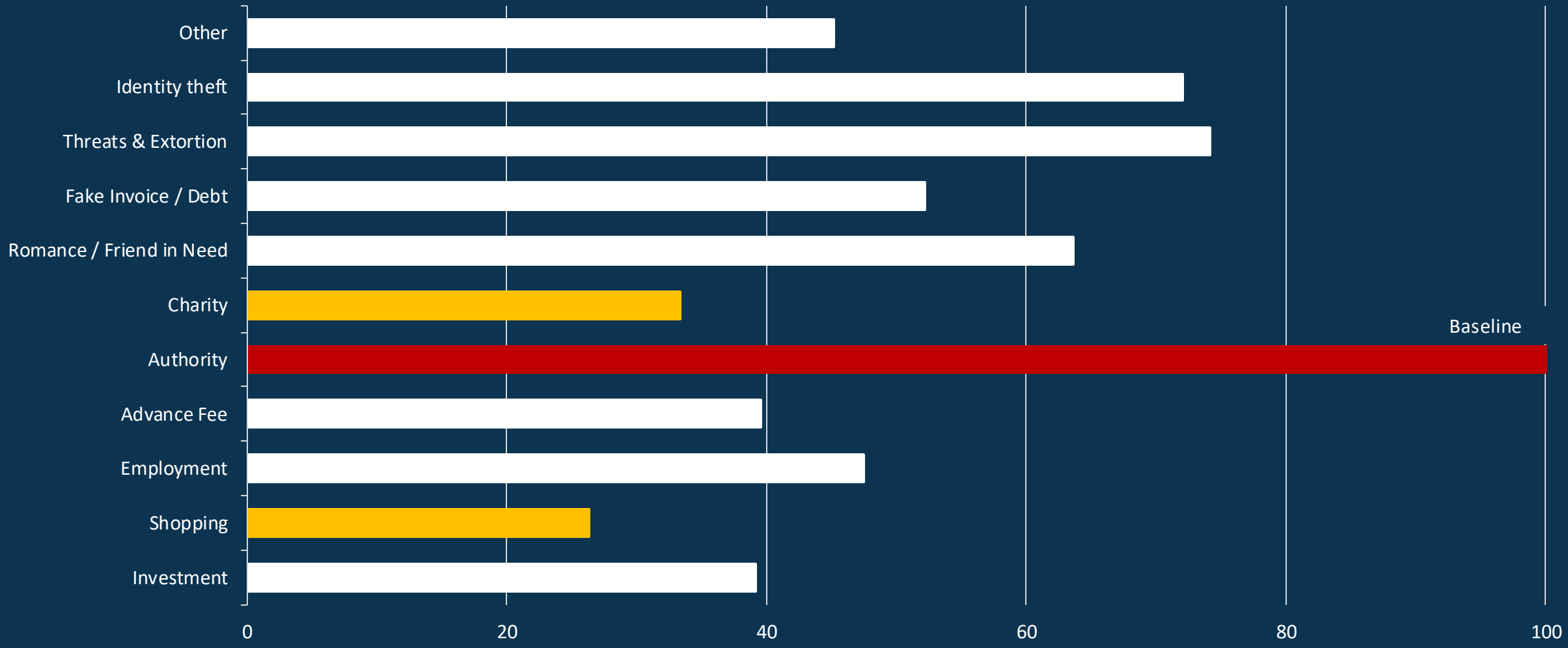
Men report scams 1.05 times more than women



Citizens from Egypt (82%), Russia (79%) and the Philippines (75%) report the least scams to Law Enforcement. Chinese (57%), Taiwanese (49%), Singaporeans (47%) and Malaysians (45%) are reporting the most.

Q10: Regarding said experience, did you report the incident to law enforcement or another government authority?

Authority-related scams are reported to government authorities the most



Online Shopping scams and Charity fraud are the least reported.

Q10: Regarding said experience, did you report the incident to law enforcement or another government authority?

Danish Registry Punktum dk A/S Reports Surge in Investment & Crypto Scams

Denmark is well-known for its rich history, sustainable urban solutions, and its quality of life, but even the Danes are not immune to the challenges posed by the digital age. Scams are becoming more prevalent, and **Punktum dk A/S**, as the responsible party for the entire Danish domain (.dk) registration landscape, has been at the forefront of these challenges. We sat down with **Jakob Truelsen, CEO of Punktum dk A/S**, to discuss the state of scams in Denmark and the efforts being made to combat them.

Denmark has a reputation for being ahead of the curve when it comes to technology. However, with this advancement, there are always those who seek to exploit it. Jakob, how significant are scams in Denmark today? In recent times, Denmark, like many other technologically advanced nations, has witnessed a significant rise in scams, especially those leveraging technology. Digital innovations, while advantageous, have also provided a fertile ground for scammers. The surge in investment and cybercurrency scams is especially concerning. As digital currencies like Bitcoin and Ethereum gain wider acceptance, there's a growing segment of the population eager to participate, often without a clear understanding of the risks. Scammers are exploiting this gap, crafting sophisticated schemes to dupe both seasoned investors and novices alike.

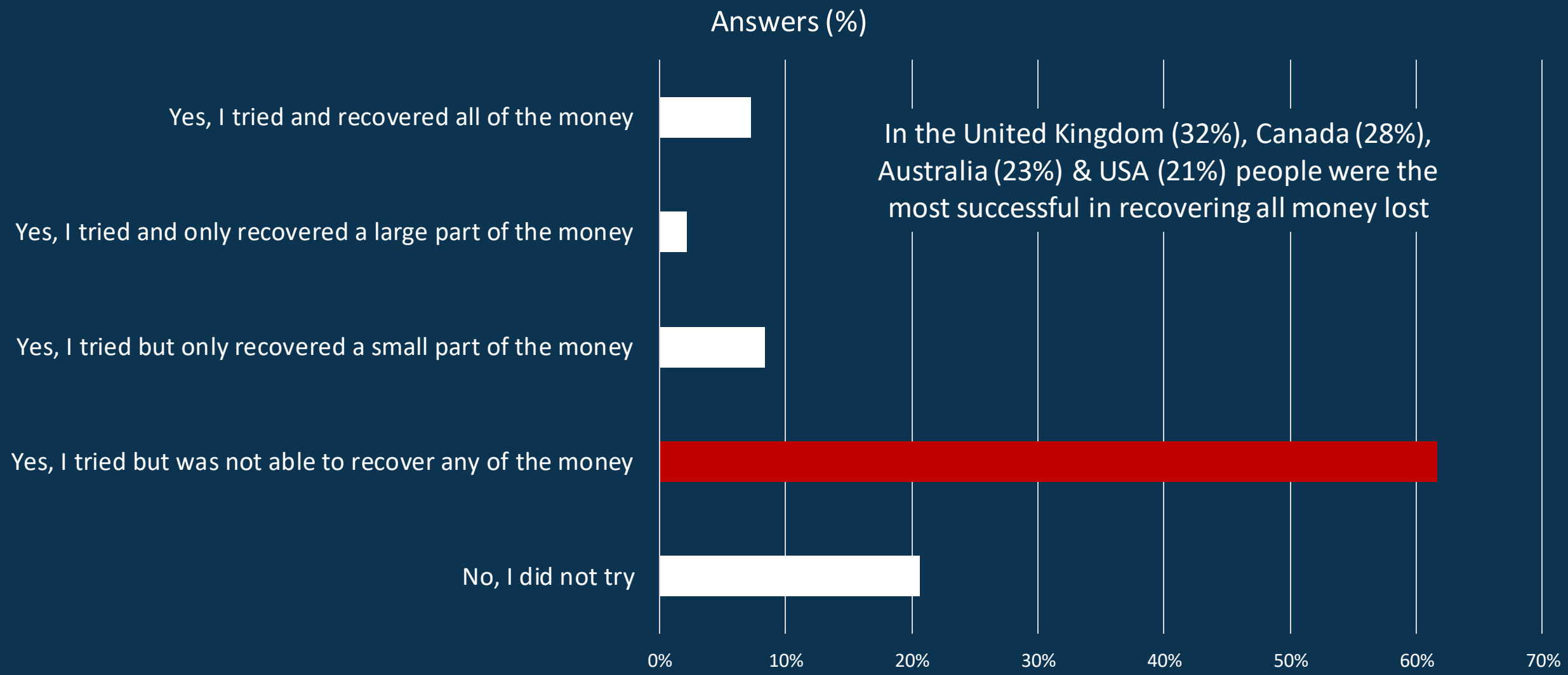
It's a disturbing trend. While we understand that there isn't specific data on "trendy" scams, could you shed light on any significant preventive actions taken by Danish organizations or the government? The Danish authorities and organizations have recognized this escalating problem and have been proactive in their response. To begin with, a range of recommendations have been issued targeting different sectors, ensuring that businesses and public institutions alike have guidelines to follow. The tool, Sikkerpånettet.dk, exemplifies this proactive approach, allowing entities to assess their vulnerability and adherence to recommended safety protocols. Additionally, at Punktum dk A/S, our commitment to bolstering the cybersecurity framework is evident. Our focus on enhancing the number of domain names with DNSSEC ensures a more secure digital landscape. Through collaborations with registrars, the achievement of a 65% record of domain names under DNSSEC is a testament to these efforts. And it's worth noting that the efficacy of these measures is amplified by the active use of DNSSEC codes, with ISPs in Denmark covering around 80% of the digital terrain.

That's commendable progress. Jakob, looking ahead, what would you advocate for in ensuring consumers remain ahead in the fight against scams? The road ahead demands a two-fold strategy: transparency and empowerment. We must prioritize efforts that shed light on the operations and entities behind these scams. While it's essential to have stringent cybersecurity measures in place, it's equally crucial to arm consumers with the knowledge and tools they need. This includes developing and promoting tools that allow users to discern the legitimacy of domain names, emails, or any digital communication they encounter. The future of digital safety lies not just in building robust defenses but also in fostering an informed and vigilant digital community. We strongly believe that we all have a responsibility, to help with information, knowledge, and tools. At Punktum dk, we carry our share of this. We are determined to combat scammers through registrant ID control and online tools like **tjekpånettet.dk** and **sikkerpånettet.dk**.

With challenges come opportunities. As scams become more intricate, Denmark, backed by organizations like Punktum dk A/S, remains resolute in its commitment to fortify its digital space, ensuring a safer digital experience for its residents.

Jakob Truelsen
CEO
Punktum dk A/S

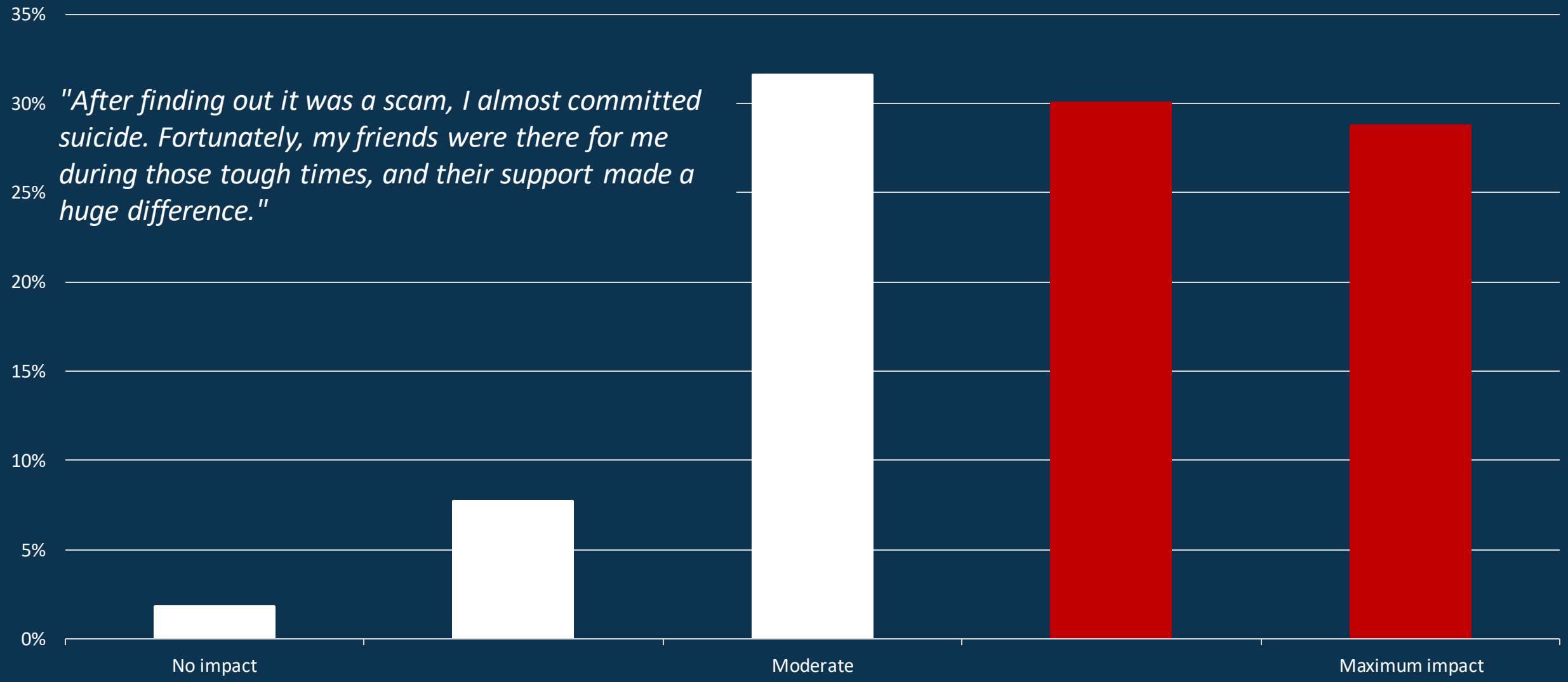
Globally, only 7% of the participants were able to recover all money lost



21% did not try to recover their funds. 62% tried but were unable to recover any money.
Those who do report have a 1.5 higher chance of getting their money back than those who do not report.

Q13: Did you try to recover the money you lost?

59% of the scam victims perceived a (very) strong emotional impact

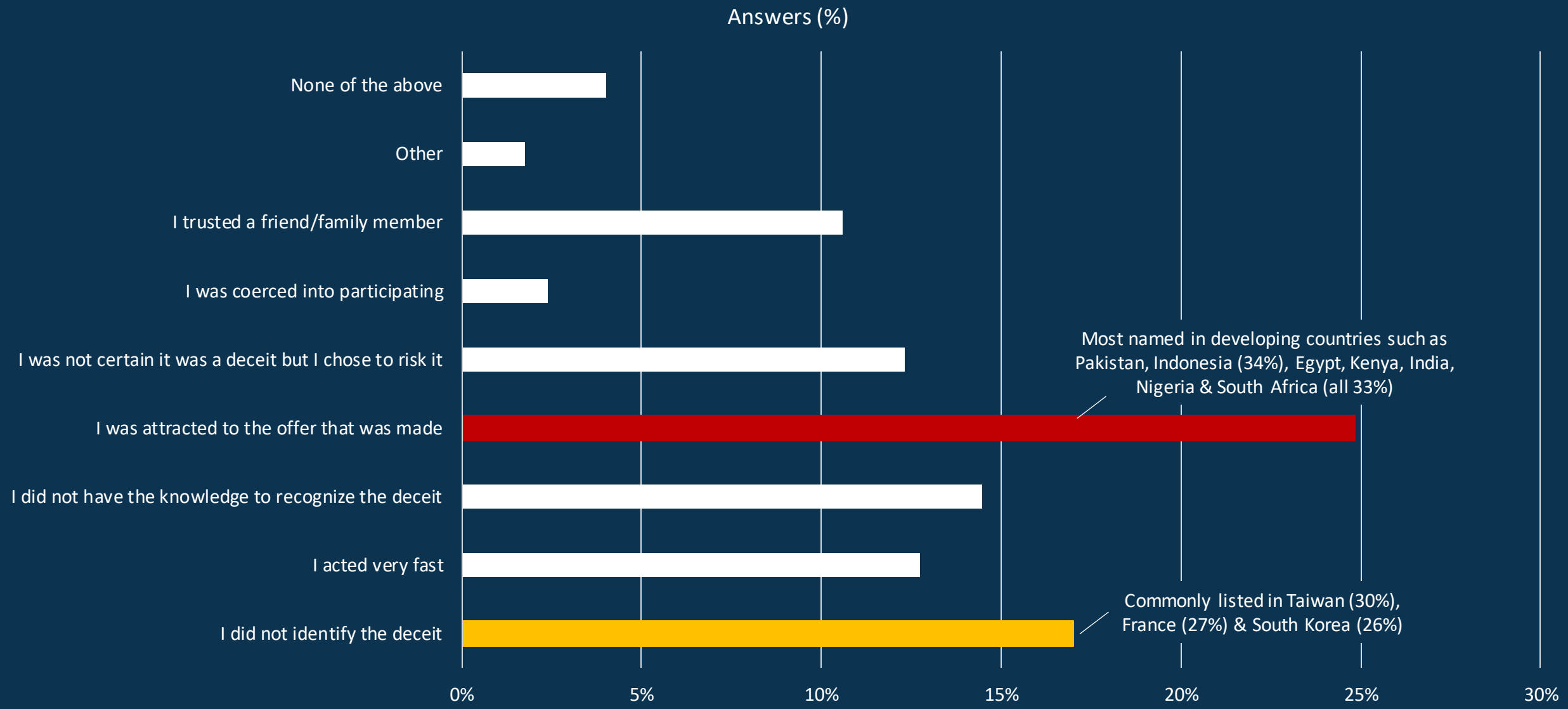


"After finding out it was a scam, I almost committed suicide. Fortunately, my friends were there for me during those tough times, and their support made a huge difference."

Only 9.6% of the participants reported little to no emotional impact.

Q14: Think about the incident that has had the most impact. To what extent did it affect you emotionally?

The main reason people are scammed is being confronted by an attractive offer



However, not identifying the deceit or lacking the knowledge to recognize the scam take a close second and third place.

Q15: You stated losing money or personal/financial information in a deceit. What was the main reason this happened?

A United Front: Harnessing Collective Power to Combat Digital Scams in France

We now turn our attention to France, a country witnessing a significant surge in online fraudulent activities. Today, we are in conversation with **Minh-Ha Nguyen**, the **Secrétaire Générale** of **Signal Spam**, an organization at the forefront of combating email spam and phishing scams in France. Nguyen investigates the rapidly evolving landscape of scams in France, sharing data and insights gathered from Signal Spam's extensive monitoring networks.

Minh-Ha, we've noticed that scams have been on the rise globally. Can you shed some light on how France has been affected? Scams have been evolving & growing not just globally, but also here in France. Over the years, we've observed a significant spike in various types of online scams including phishing, smishing & banking scams, with emails & texts being the primary scam mediums. At Signal Spam, we've seen about 3.2 million reports classified as "phishing" by internet users in the past year. In 2022, the top three reported campaigns were parcel delivery scams with 364k reports, CPF scams with 140k reports & police summon scams with 38k reports.

What kind of scams that were trending in France last year? Scammers tend to adapt quickly to current events. Last year, we saw a nationwide malicious campaign that tricked people into fake health security card renewals to collect their personal data & credentials. Following the global energy crisis & concerns about climate change, scams offering state subsidies for energy retrofits also multiplied. The "Compte Personnel de Formation" (CPF) scam proliferated widely, exploiting the government's initiative to support personal training & skill development. Another prevalent scam was the parcel delivery scam which escalated since the pandemic, utilizing emails, text messages & even fake QR codes sent directly to people's letterboxes. And of course, the fake police summons scam that spread massively between 2020 & 2022, with countless fake summons sent via email.

It seems like a significant issue. What steps have the French government & other organizations taken to protect consumers? Yes, it's a growing concern. Our government & several organizations are actively working to safeguard consumers – **PHAROS**, **THESEE** & **Perceval**. They have introduced official online services where people can report scams & file complaints. We also have online platforms like **Cybermalveillance.gouv.fr** & nonprofits like **Signal Spam** & **33 700** where people can report emails & smishing, respectively. There's a special police unit focusing on combating online malicious acts too. A lot of effort is being invested in education & communication initiatives to raise public awareness about cyber threats. In fact, October has been designated as CyberMonth in France, bringing together a wide range of stakeholders to share advice & best practices for cybersecurity. And on the legislative front, a new bill is under review to secure & regulate the digital space better, including the creation of a national anti-scam online filter.

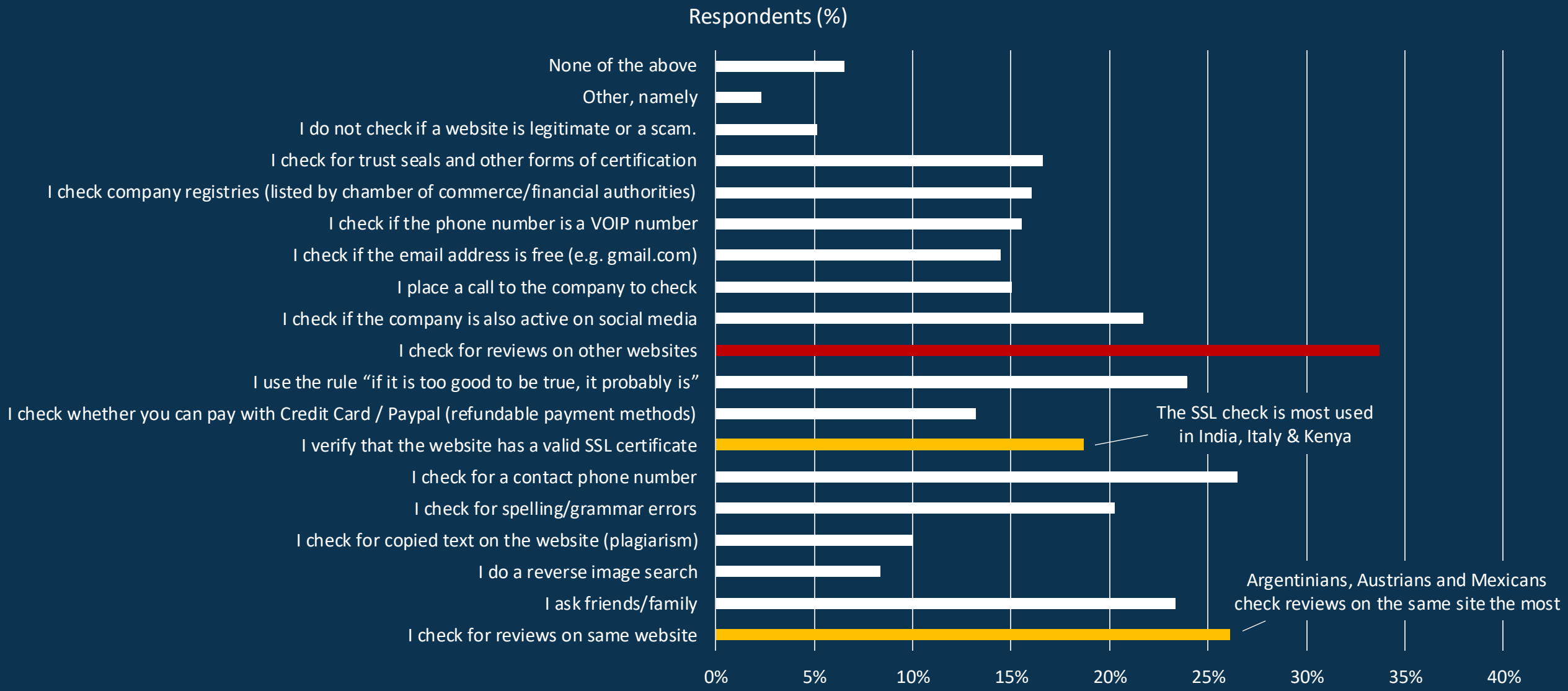
Can anything be done to give French consumers an upper hand in this battle against scams? Empowering consumers is vital in this fight. Firstly, we need to launch comprehensive education & awareness campaigns to inform the public about common scam tactics & how to recognize them. Secondly, we must enforce strict regulations to hold platforms & financial institutions responsible for facilitating scams. Developing advanced AI & machine learning technologies for scam detection & prevention could be a significant step forward. Moreover, encouraging a culture of reporting scams & collectively sharing information can strengthen our defenses greatly. The EU's DSA directive is a great blueprint for such regulatory measures. I firmly believe that these actions can indeed give consumers the upper hand.

Minh-Ha gives us hope that through unity, awareness, and technological advancements, France can forge a potent shield against an ever-advancing scam threat.

Minh-Ha Nguyen
Secrétaire Générale
Signal Spam

signal spam

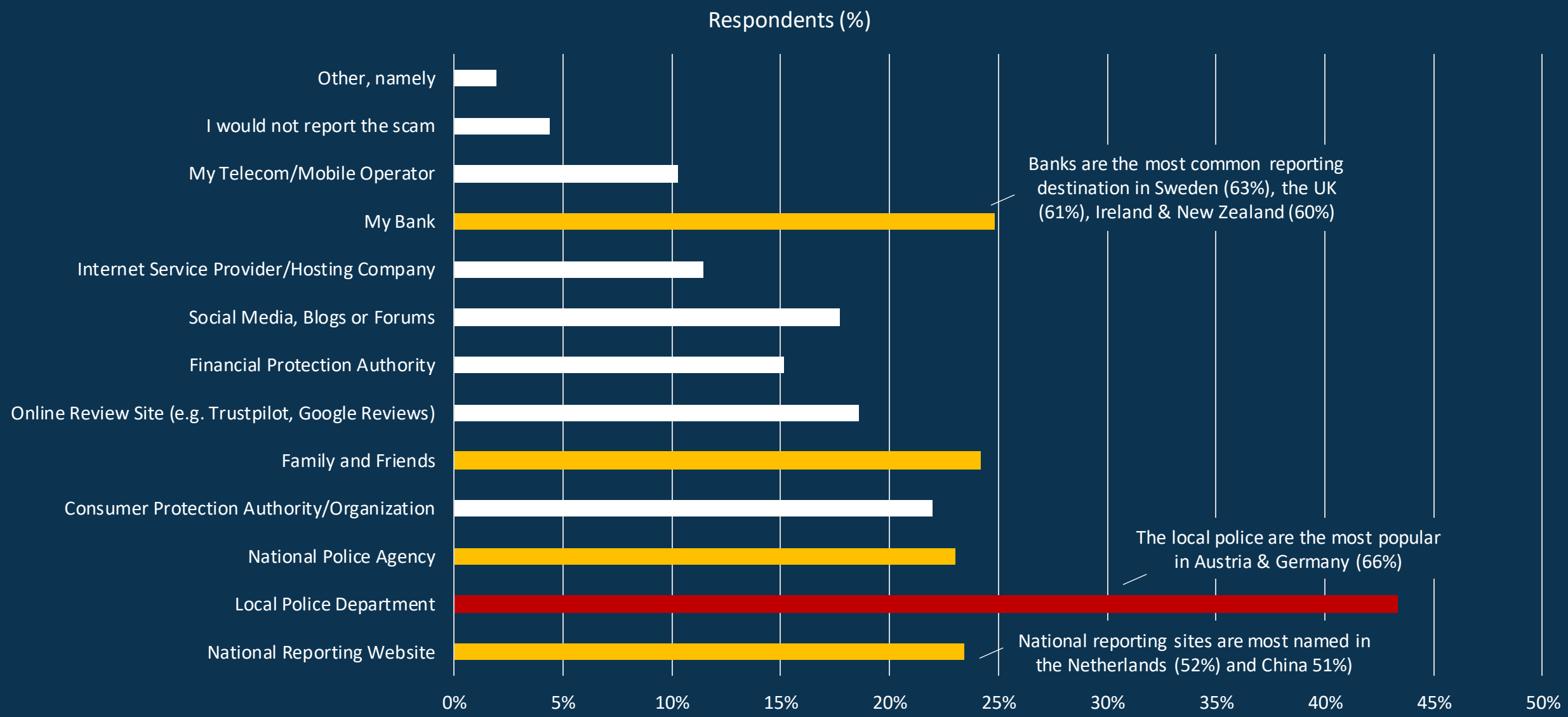
The most common way to check for scams is reviews on 3rd party sites



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

Q16: Which methods do you usually apply to check if an offer is legitimate or a scam? Select all that apply.

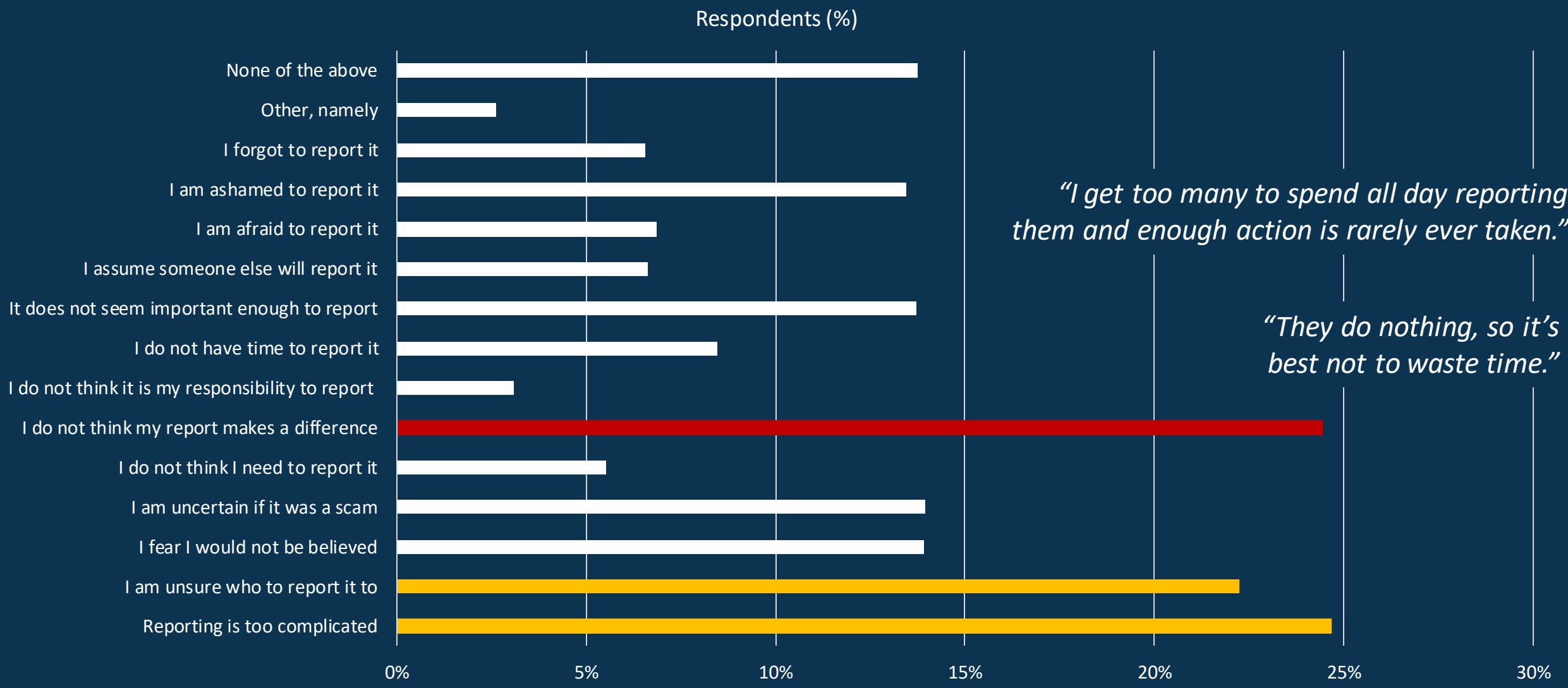
Scams are mostly reported to the Local Police Department (43%)



Followed closely by Banks (25%), Family and Friends (24%) and National Police / Reporting Sites (23%).

Q17: If you were to be deceived, who would you report this to?

24% of participants believe reporting a scam would not make a difference



"I get too many to spend all day reporting them and enough action is rarely ever taken."

"They do nothing, so it's best not to waste time."

Other key reasons for not reporting are that reporting is perceived as too complicated (24%) and uncertainty where the scam should be reported (22%).

Q18: What reasons might you have to not report a scam?

Australia Fights Back with National Anti-Scam Centre & Cross-Industry Standards

In Australia, the fight against scams is in full swing, as government and industry coordinate efforts to curb the menace and protect citizens from predatory tactics. We bring you insights from **Heidi Snell, the Executive General Manager of the National Anti-Scam Centre at the Australian Competition & Consumer Commission (ACCC)**. Here, she explains the current state of scams in Australia, the trends in 2022, and the government's robust strategy to tackle this issue head-on.

Can you give an overview of the extent of scams in Australia according to recent data and the effects on victims? Absolutely. The 14th annual Targeting Scams report by the ACCC highlighted that in 2022, scams accounted for over $3.1 billion in losses. The figures have been rising steadily since 2020, with Scamwatch recording $569 million in losses last year, a stark 80% rise from 2021. Unfortunately, this year we have already witnessed a 44% surge in reports, with losses approximating $351 million. The repercussions for victims are substantial, with the average loss in 2022 soaring by 54% to nearly $20,000, resulting in a long and difficult recovery process.

Which scams stood out the last year in your country and were "trendy"? Last year, ***investment scams*** were predominant, particularly those facilitated via phone and social media, with cryptocurrency being the common payment medium. ***Bank impersonation scams*** were also rampant with 14,603 reported cases, where scammers would pretend to be calling from a bank's cybersecurity or fraud department. ***Employment scams*** have risen substantially, with scammers exploiting social media to offer faux work-from-home opportunities, usually associating themselves with legitimate companies and promising substantial earnings for minimal effort. Furthermore, ***impersonation websites*** mimicking renowned retail brands emerged to trick consumers into revealing their credit card details or paying for undelivered goods. In terms of scam contact methods, ***text messages*** surpassed phone calls as the primary contact method, registering an 18.8% increase on the previous year.

Which actions have been taken by your government and other organizations to protect consumers from scams? Any best practices from which we can learn? To counter the increase in sophistication of scams, the Australian government establish the National Anti-Scam Centre on 1st July 2023 focusing on a whole of ecosystem approach to scam prevention and detection. It brings together government and private sectors to thwart scams through data & intelligence gathering, disruption through fusion cells, and enhancing public awareness and education. Australia has implemented codes to minimize scam calls & messages and is developing a registry to block scam texts impersonating well-known organizations. Some parts of the financial sector introduced initiatives such as payment delays, name & account matching, blocking high-risk crypto platforms and real-time scam account data sharing.

What further initiatives do you propose to empower consumers in their fight against scams? Moving forward, we aim to bridge the existing gaps in the ecosystem that make it susceptible to scams. We advocate for the establishment of mandatory and enforceable cross-industry standards that encompass not just banks but also telecommunications, digital platforms, and cryptocurrency exchanges. Collaborative efforts with relevant stakeholders will be pivotal in building a scam-resilient ecosystem.

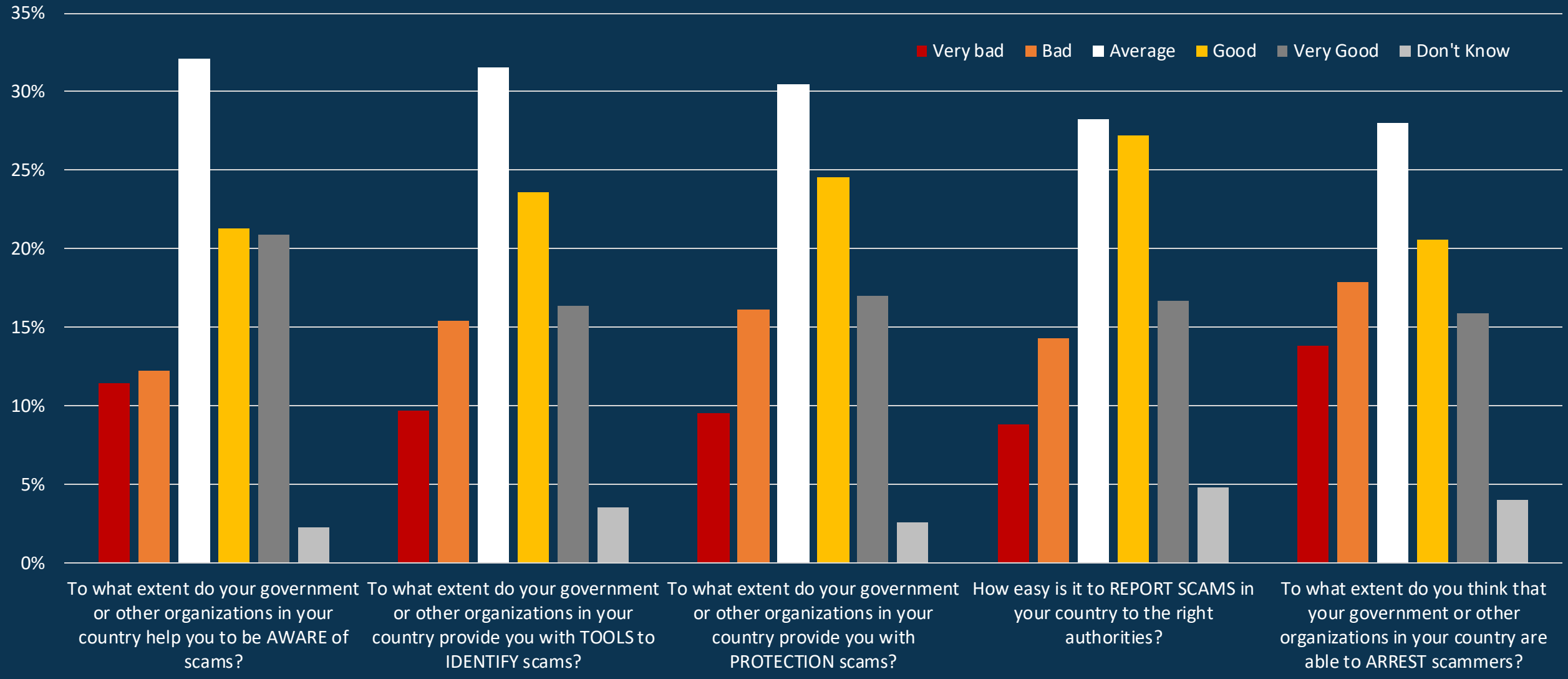
With cohesive efforts from government and private sectors, Australia aims to cement a resilient digital ecosystem, safeguarding its citizens from scams. Heidi Snell's insights reflect a steadfast pledge to adapt, take action, and to ensure Australians look forward to an increase in security and prosperity.

Heidi Snell
Executive General Manager
National Anti-Scam Centre at the Australian Competition & Consumer Commission

Australian Government

National Anti-Scam Centre

Globally, people are displeased with the number of scammers getting arrested

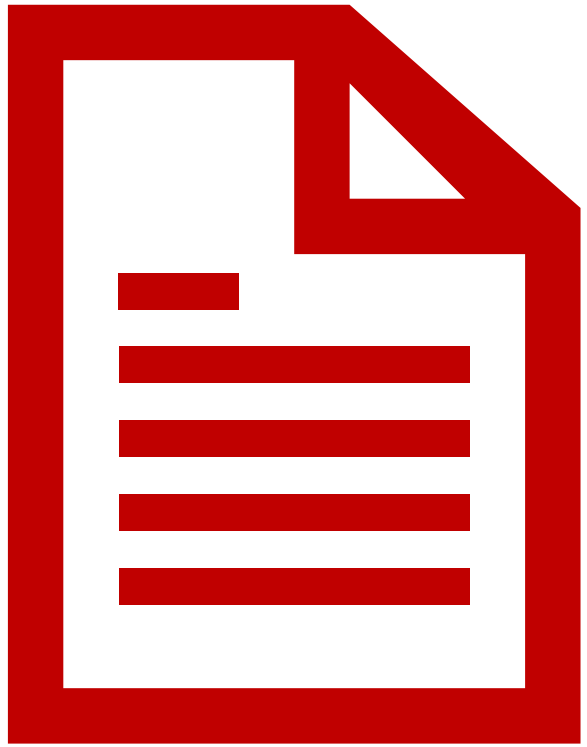


Across all perspectives, the authorities in Brazil and Thailand are regarded as least capable regarding online fraud. Their counterparts in Saudi Arabia, United Arab Emirates, and China are rated the best by their respective populations.

Q19: How would you rate the efforts of your government and other organizations in your country in fighting online scams?

SCAMADVISER

About this Report



GASA
Global Anti-Scam Alliance

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.

ScamAdviser.com checks the likelihood of a website being “legit or a scam” for more than 6.5 million consumers monthly. More than 1.5 million new domains are added to its database every month. Via its Data Partners, ScamAdviser protects more than 1 billion consumers worldwide.

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, Jack Whittaker, PhD Candidate Criminology at the University of Surrey and Peter Hagenaars of the Dutch Police, for their feedback and support.

Methodology

We used Pollfish.com to set-up the consumer survey and get participants. Pollfish utilizes 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.

Biases towards a specific age or educational level were statistically corrected based on the general distribution within a country. The estimate how much money was lost remains a difficult question to answer. Depending on the country outliers had to be removed. Also, for bitcoin, it was not possible to report amounts smaller then 1. Hence bitcoin loses were not included in the estimate.

In addition to Pollfish we used the following sources:

- Inhabitants per country: Worldometers.info
- Currency conversion: Xe.com
- The country flag on the cover: wikimedia.org
- Internet penetration: Wikipedia
- GDP Estimate 2023: Wikipedia

The survey itself has been party 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.

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

amazon | Gogolook | SCAMADVISER | TREND MICRO

Corporate Partners

AnyDesk | BARCLAYS | BioCatch | cifas (Fighting Economic Crime Together) | cira | Crystal

CSC | EBRAND | eu Powered by EURid | feedzai | globaleyez the brand protection experts | GROUP-IB

LexisNexis RISK SOLUTIONS | mastercard | REALTIME REGISTER

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

SCAMADVISER

Disclaimer

This report is a publication by the **Global Anti-Scam Alliance** (GASA) supported by **ScamAdviser.com**. 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

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

GASA
Global Anti-Scam Alliance