

callsign[®]

WHITEPAPER
SERIES



Global scams report

The damaging impact of consumer
scams on reputation and revenue

MAY 2023



GLOBAL SCAMS REPORT

Executive summary

It's not a shock to say that consumer scams are on the rise. But by surveying both financial institutions (FIs) and consumers, Callsign's unique global perspective has identified four key new and future trends for fraud teams to be aware of.



There is a scams language gap between FIs and their consumers

- FIs need to think in the language of their consumers, and the lack of a common language in scams terminology runs the risk of isolating consumers who are labelling scams differently to FIs
- Reliance on internal fraud classifications could be impeding effectiveness in scam prevention and education



2 FIs need to rethink their fraud strategies to fit the current and future scams landscape

- 44% of FIs told us they find it difficult to measure and understand what is effective in combating scams
- The scams landscape has changed, and investment in fraud and threat detection alone won't protect consumers from the rise of authorized fraud



3 Scam prevention should be segmented by age and channel

- Globally, social media is the top channel where scams occur, and this is only set to grow as more young people get online
- Young people are being scammed more than any other age group



4 The impact of scams on organizations' reputations has a direct impact on their revenue growth

- Nearly 1/3 of consumers said they would stop using a bank or company associated with a scam
- 67% of FIs said they faced customer retention challenges after being associated with an online scam

We've been tracking trends and the growth of online scams, and in this paper we can expose the exponential global explosion of scams across different attack vectors and geographies.

This paper will outline the unique perspective we have on consumer scams with the data we have gathered from both FIs and consumers. We have uncovered can reveal the reputational impact scams are having on businesses, and why we believe that a layered and dynamic approach across entire customer journeys is the best way to fight scams – and to protect businesses and their consumers.

SECTION ONE

The complicated scams landscape

There is a fundamental language gap between FIs and consumers when it comes to talking about scams.

Our research found that consumers classify all types of fraud as a 'scam', not distinguishing between authorized and unauthorized types. Consumers cite a huge range of fraud types as a scam, such as phishing for PII data, romance scams, bots or malware, and investment fraud. By contrast, FIs typically only consider authorized fraud to be a scam – but even this will vary between individual FIs and across regions. This makes education and prevention difficult, because what consumers perceive a scam to be, may be classified as something different within fraud teams. The confused terminology can result in a lack of clarity for FIs when it comes to investing in solutions.



FIs need to start talking in the language of their consumers and avoid being at risk of solving for internal classifications rather than the reality of what consumers are experiencing

The fraud landscape has shifted, and will continue to shift, at a rapid rate – meaning that the task of categorizing new and numerous fraud types will be overwhelming, and a potentially inefficient use of fraud teams' time. Further to this, there is a reputational risk of rigidly adhering to fraud classifications when liaising with consumers. A consumer may reject the idea that they 'authorized' a fraud attack when they were manipulated into it by a scammer and the implications of their actions were unknown. The language used to describe scams needs to be more accessible to consumers, particularly since both consumers and fraud teams must be united in the fight against scammers.

The increase in volume of both scam messages and scams themselves has blurred the lines as to what constitutes unauthorized and authorized fraud. Scams are no longer just a one-step attack or linear. For example, phishing is not just deployed for unauthorized fraud; our data shows the growth in telephone fraud, and news headlines abound with stories of phished credentials used to gain consumers' trust for social engineering and authorized fraud scam attacks (such as APP).

Our fraud diagram shows the different activities described by consumers as scams, and then the paths that a scam can take, encompassing authorized and unauthorized fraud. An individual can be socially engineered via a multitude of methods to acquire their personally identifiable information (PII), which the fraudster then uses to either commit unauthorized fraud (e.g., ATO), or to gain someone's trust and coerce them into making an authorized payment.

Harvesting information - wants security credentials and personally identifiable information (PII)



'Social Engineering'
(enabler underpins)

Methods used to obtain the information



Phishing
emails & links)



Smishing
(text messages)



Vishing
(voice messages)

The two main types of fraud vectors used to obtain payment



Account Takeover
unauthorized fraud



Authorized push payment
authorized fraud

Types of scams² used by fraudsters



RATS



BOTS



**Romance
scams**



**Investment
scams**



**Purchase
scams**



**Card payment
scams**

¹ **Social engineering definition:** the context of information security, the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

² **A scam** is used to cheat someone out of something, especially money. Scam is also a verb meaning to cheat someone in such a way. Example: Banks will never call you asking for your credit card number or social security number over the phone

SECTION TWO

Global trends

Across the globe online scams have grown rapidly, but in the past year alone the increase is staggering.

**45%****of the consumers we surveyed said they had lost money to a scam in the past**

These losses are spread across a variety of scam types, from romance to phishing and APP fraud, reflecting the broad sweep of fraud types that are inundating digital life.

It may not be a surprise that phishing is still so prevalent, but the volume of scam messages that consumers receive may be. In 2021, 40% of consumers had seen a scam message across at least two online communication channels which we asked about. However, in 2022 that number had increased to 68% – an increase of 70%. It's worth noting that in the UK and Singapore, only 17% and 16% of consumers respectively said they hadn't received a scam message via SMS, indicating the huge scale of scams being sent via SMS.

While the overall volume of scams has increased almost uniformly across digital channels, our research has further indicated a shift on a global level towards social engineering and coercion as a way to execute authorized fraud – with phone calls made by scammers to consumers increasing by almost one third.

With many of these scam types leveraging scam messaging to target consumers, scams and scam messages will continue to rise.

Future scam trends

Interestingly, the top channel for receiving a scam message in the UAE was on messaging apps (such as WhatsApp or Facebook messenger). Elsewhere, email was highest in the UK and US, and SMS was the highest across multiple countries in APAC, for example in the Philippines, Singapore, and India.

Figure 1: How consumers lost money in a scam

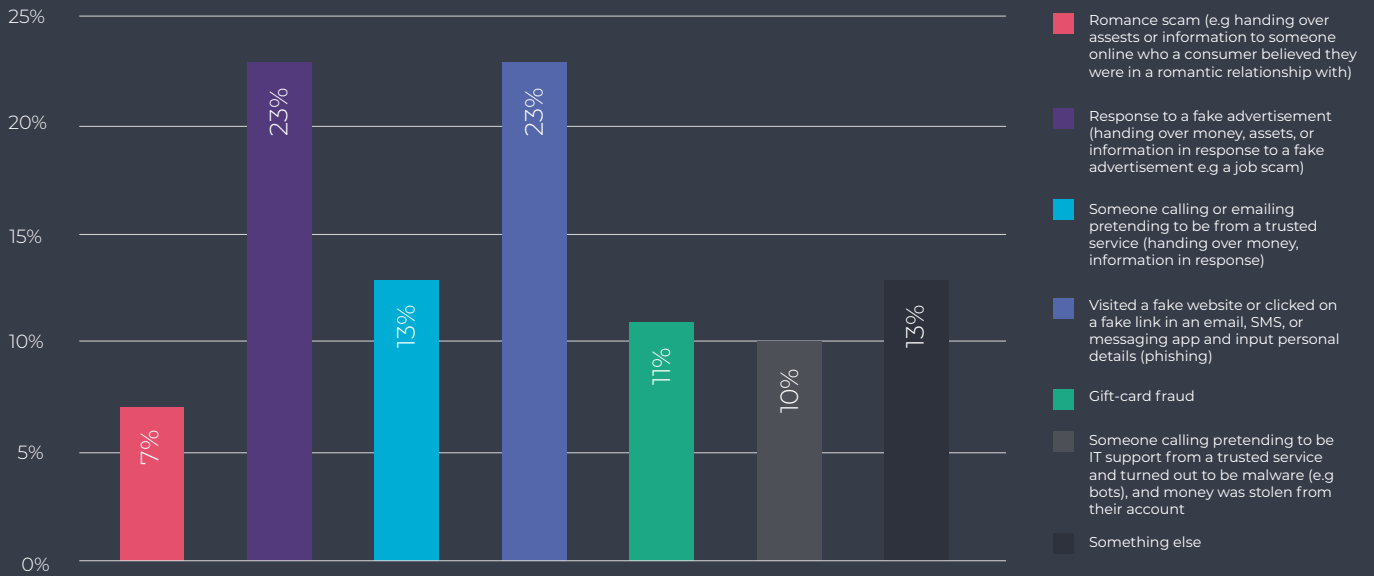
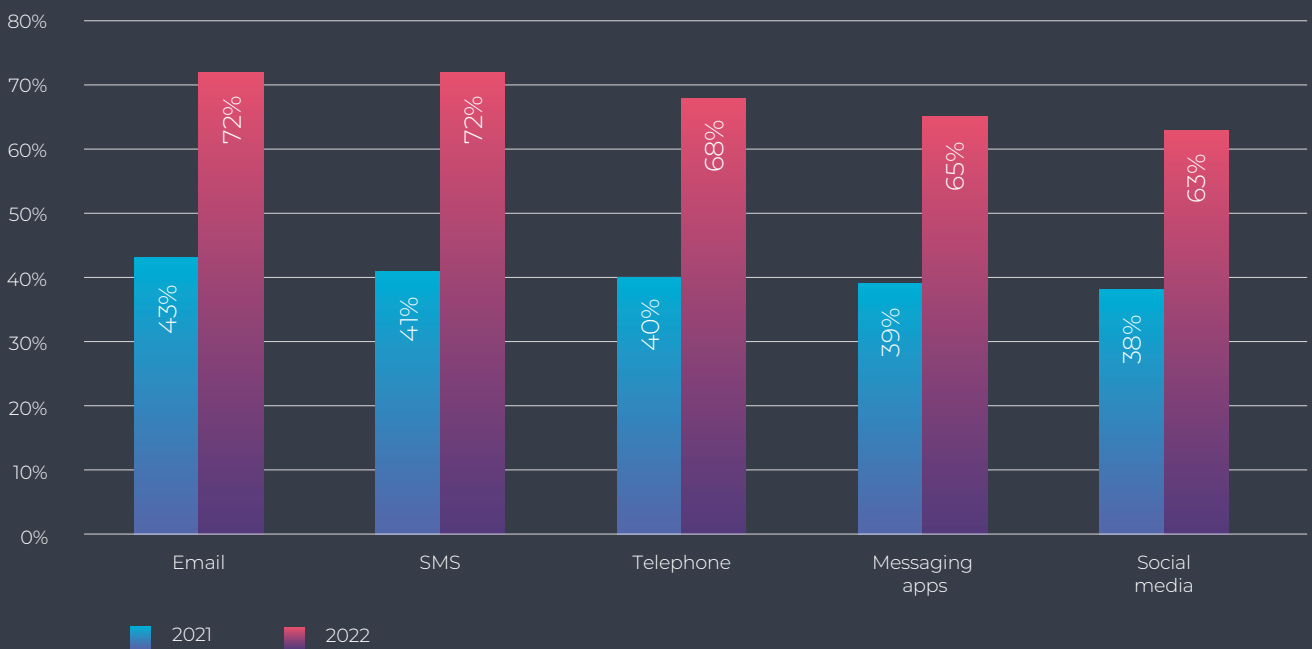


Figure 2: The rise of scam messages



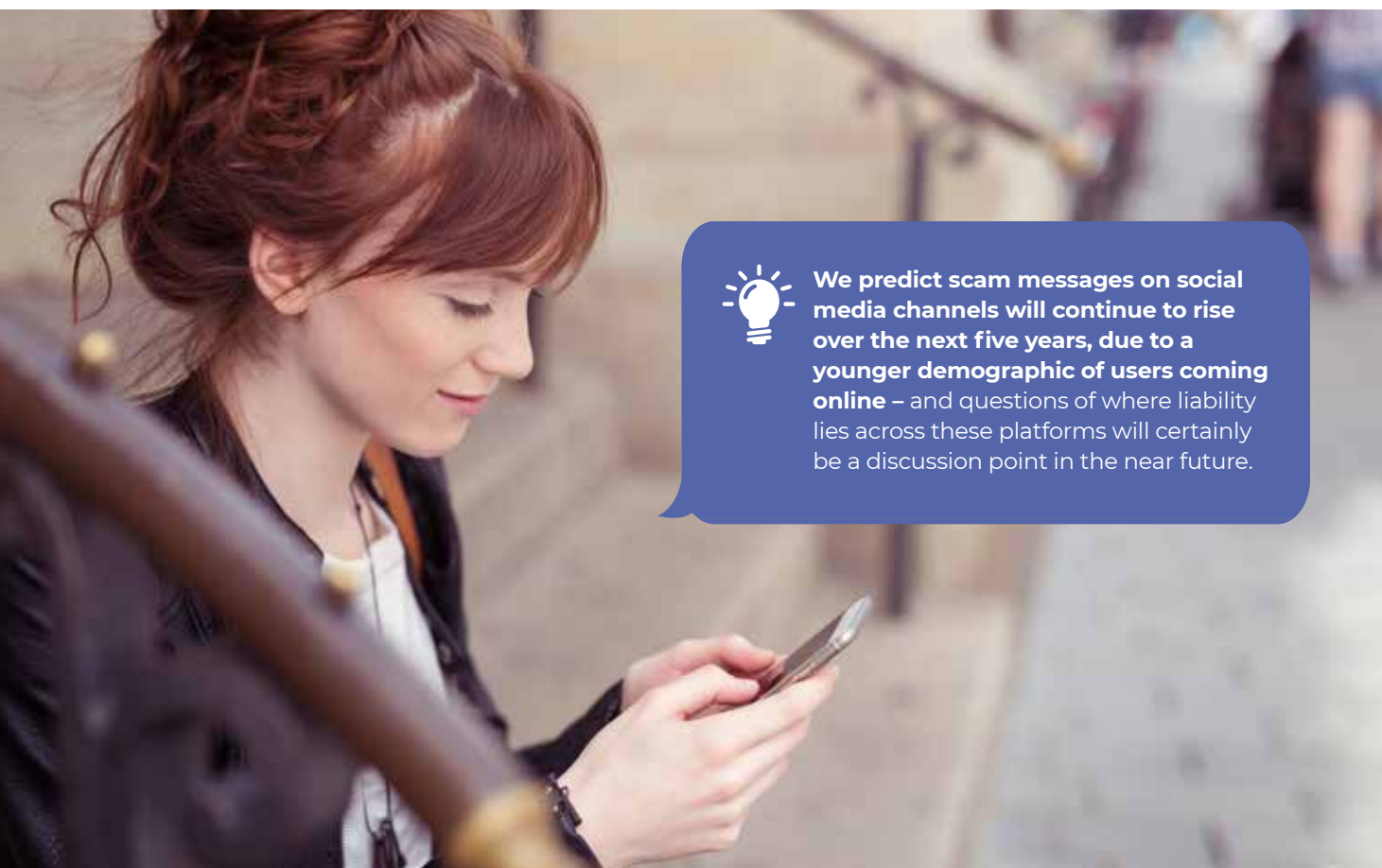
This regional data point from the UAE is indicative of a wider global trend. Our research revealed that **one in three consumers who were scammed cited social media as the channel it happened on**, making it the most successful channel for scams to happen on.

And the rise in scams on these channels also helps to explain why there is a gap in the generational experience of scams.

We found that 31% of 18–34-year-olds have seen a scam message on social media, compared with only 13% of over 55s, and on messaging apps 35% of 18–34-year-olds have seen a scam message versus only 17% of over 55s.

By contrast, over 55s have seen a scam message most often on email (48%) or via the telephone (45%). Scams don't target consumers in a uniform way, and different age groups are susceptible to different channels and vectors – adding to the complexity of the task of preventing them.

In conclusion, young people are more likely to fall for a scam than the older generation – 59% of 19–34-year-olds have fallen for a scam compared to 36% of those over 55, and the prevalent use of social media by younger generations might explain this trend.



We predict scam messages on social media channels will continue to rise over the next five years, due to a younger demographic of users coming online – and questions of where liability lies across these platforms will certainly be a discussion point in the near future.

Scams erode digital trust

In the ever-growing digital world, online scams are quickly eroding digital trust between consumers and organizations. **Scams challenge the confidence that consumers have about who they are interacting with in the digital world.** Consumers must be vigilant about messages they receive online, constantly questioning if a message is genuine or fraudulent.

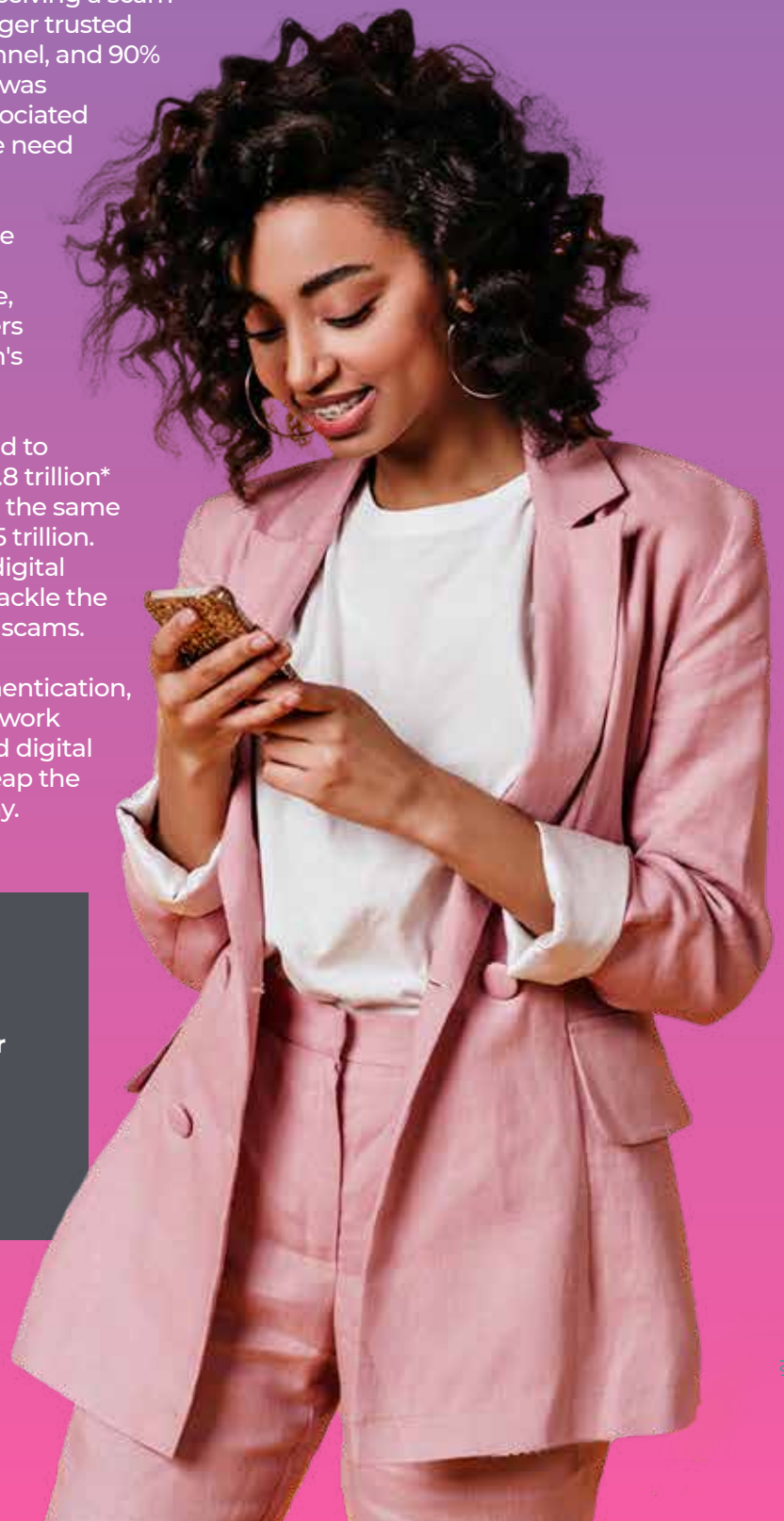
Consumers (79%) told us that after receiving a scam message on any channel, they no longer trusted messages they were sent on the channel, and 90% said their trust in a company or bank was changed when the company was associated with a scam in the news. FIs therefore need to be aware that scammers are using the very same channels that they themselves are using to communicate to their customers. This erodes trust in the channels used to communicate, and this makes it harder for consumers to have confidence in an organization's ability to protect them.

While the digital economy is expected to grow from \$14.5 trillion in 2021 to \$20.8 trillion* by 2025, the cost of online crime over the same period will rise from \$6 trillion to \$10.5 trillion. If businesses want to gain from this digital economic growth, they will need to tackle the breakdown of digital trust caused by scams.

This puts the spotlight on fraud, authentication, and digital teams, and how they can work across their organization to help build digital trust so that their organization can reap the benefits of a growing digital economy.

 79%

of consumers told us that after receiving a scam message on any channel, they no longer trusted messages they were sent on the channel



SECTION THREE

The cost of scams

The top and bottom line

Ensuring growth in the digital economy is critical for an organization's commercial survival, and so we wanted to understand how different FIs are responding to the constant threat scams pose for their customers.

Callsign commissioned Forrester Consulting* **to conduct a survey of senior decision-makers from financial organizations** across the globe to get their perspective on the risks scams pose for their businesses.

FIs stated that consumer scams have a significant impact on their bottom-line growth. Lost productivity (74%) and increased back-office expenses (76%) were both cited as key challenges that scams create for their business.

But FIs also recognized that their top-line growth is impacted by consumer-based scams too. Bad publicity and reputational damage (74%) and the inability to attract new customers (75%) were critical areas of concern for businesses. The hit to both top and bottom-line growth means that overall, 62% of businesses we surveyed attributed 1-6% of lost revenue due to consumer-based scams, and 13% lost more than 11% in revenue.

Damage to brand reputation

Organizations are right to recognize the detrimental impact scams have on their brand. The multiplier effect of a scam is huge, with nearly a quarter of consumers complaining about the company on social media and almost half telling friends, colleagues, and their family. A single scam can have a huge reach, damaging the reputation of FIs and having lasting effects.

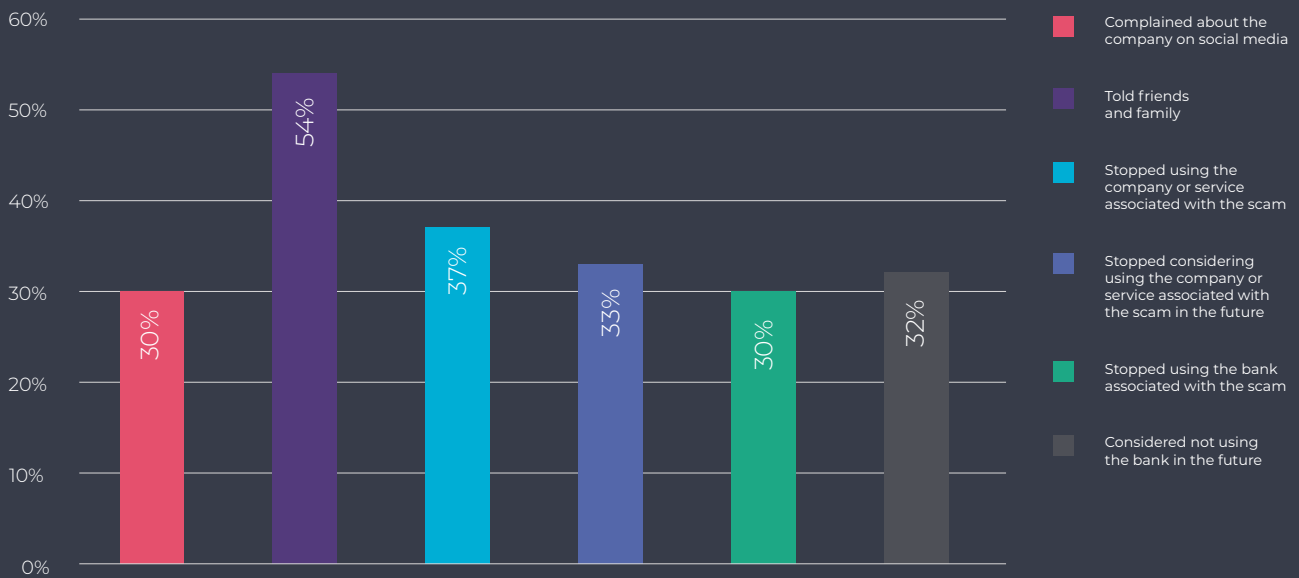
We asked consumers what they did after receiving a scam message, reading about a scam, or having been scammed. The results are worrying for all organizations.

For those who fell for a scam, the most common response was to tell friends, colleagues, and family (47% of respondents), followed by 33% of people who said they stopped using the company or service whose name the scammer used in the scam message. This data demonstrates that even simple brand association with a scam has lasting impact on the business.

**33%****we found a third of consumers who fell for a scam choose to stop using that company**

For those consumers who haven't fallen for scams, they still had a strong response to simply seeing a company or bank they used associated with a scam. Nearly a third of consumers said they would stop using a bank associated with the scam, and a third said they would stop using the company associated with the scam.

Figure 3: Consumers' response to seeing a scam message




Our research also revealed that when choosing who to bank with, the top two factors influencing consumers' choices were a bank's ability to protect them from becoming a victim of scams or fraud, and their ability to protect their privacy bank with.


Consumers rely on FIs to keep them safe – and when they fail to do so their trust is broken, with little regard for the type of scam they fell for.


The research also demonstrated that businesses recognize the need to invest in scam prevention strategies: 81% say they have created a dedicated fraud and threat program, 73% stated they have increased spending on fraud detection technologies, and 65% are planning to spend more money on scam prevention strategies.

The impact of scams is like dropping a stone in a still pond, causing a huge ripple effect of damage – reputationally, revenue wise, and potentially legally, with multiple governments and regulators looking at how to better protect consumers through legislation.

Businesses are aware that brand association with a scam is damaging. When asked about the impact that online scams have on their reputation,

 **71%**
of business leaders were worried about poor online reviews

 **68%**
were worried about negative press / media coverage,

 **67%**
of business leaders said they faced customer retention challenges

SECTION FOUR

What is the solution?

Unfortunately, 44% of organizations said they have difficulty measuring and understanding what is effective in combating fraud and scams, which can lead to investing in the wrong technology.

This is understandable, given the scale of the challenge that businesses face in protecting their customers against scams. Scams know no boundaries and operate across all geographies and channels – made more complicated by the volume of messages and range of tactics used by scammers (such as malware and bot attacks, phishing, romance scams) at all stages in the user journey.

Simply investing in fraud detection technologies, threat and fraud programs and threat intelligence capabilities is not enough. In a complicated and dynamic fraud landscape, these alone will not protect an organisation and its customers from the threat of scams.

When only looking for threats, organizations are unlikely to identify the subtle signs of when a genuine user is being socially engineered, or if a fraudster is using genuine credentials for ATO – allowing more scams and fraud to slip through the net. Traditional unauthorized fraud (ATO) has been easier to detect with threat detection, but the rise of authorized

fraud (with vectors such as APP) has made threat detection solutions less effective, since it is the genuine user authorizing payments.

What is required is a layered approach that combines the power of threat and identity models throughout the online journey. This is where Callsign can help.

Callsign has created solutions to address this challenge of tackling both authorized and unauthorized fraud. Our unique machine learning models approach to tackling scams and fraud protects both consumers and businesses at every stage of the user journey.

Callsign uses AI and has a unique approach to modelling. This includes creating a Digital DNA profile for each user in order to help authenticate them. A Digital DNA profile is made up of 40+ sub-models, each containing datapoints from behavioral biometrics, device and location intelligence to provide a panoramic view of a user with regards to their behavior. This allows Callsign to accurately identify users with exceptional granularity.

In addition to being able to identify genuine users with minimal friction, it allows Callsign to recognize any abnormal behavioral patterns. This may indicate when a user is under duress and at risk of authorized push payment fraud.



Our **Detect, Intervene, Protect** approach allows clients to tackle scams by providing contextual fraud warnings that fraudsters can't anticipate, or coach users through.

Callsign's **Orchestration Layer** allows FIs to intervene if a scam is suspected to be taking place. The Orchestration Layer gives FIs the ability to add dynamic and contextual messages in a low-code / no-code and easy-to-use drag-and-drop environment. These messages can be quickly adapted so FIs can pivot in the fast-changing scam landscape, and can be A:B tested. The Orchestration Layer also allows FIs to centralize their decision making by integrating new & existing third-party vendors.

In combination with this, our 1-to-many fraud model also uses behavioral biometrics, device, location as well as threat parameters to identify behavior typical of a fraud cohort. The model can detect specific behavioral indicators that relate to fraud, such as overly consistent machine-like typing, as well as threat inputs like a bot or RAT. This is then ensembled into a threat score which is made available via REST API.

Callsign's technology enables organizations to detect scams that can lead to both authorized and unauthorized fraud at any point in a user's online journey. With our **ATO Protection** and **APP Protection**, businesses and consumers will be protected across all scam & fraud types.





GLOBAL SCAMS REPORT

Conclusion

The global scam landscape is one which is continuing to increase in scale and is filled with complexities.

Scams are on the rise, with more channels and fraud types being exploited by fraudsters. Consumers face being overwhelmed with scam messages and being exposed to risk of monetary losses, while businesses are aware of the need to protect their reputations from the scam fallout.

A layered, agile, and balanced approach must be taken to combat online scams. Businesses must invest in solutions that can best respond to widespread and rapidly changing fraud vectors, encompassing both unauthorized and authorized fraud.



Get in touch so we can help protect your reputation & customers against scams: www.callsign.com/contact

Endnotes

¹ In December 2021, the Global GDP estimate was \$94 trillion (*Visual Capitalist*) with the *World Bank* estimating that **15.5% of Global GDP in 2021** was the digital economy, meaning \$14.5 trillion. The *World Bank* also estimates that over the past 15 years, the digital economy has grown **2.5x quicker than the Global GDP**. To calculate the value of the digital economy in 2025, we averaged global growth forecasts for 2022 from the *IMF*, *World Bank* and *Fitch Ratings*, which equalled 3.73%. Given that the digital economy grows 2.5x quicker than Global GDP, the digital economy's growth rate for 2022 was 9.33%. Compounding this growth until 2025 meant that the digital economy would be worth \$20.8 trillion.

Appendix

Scams data 2022 - Research was carried out in partnership with Opinium. The total sample size was 8000 adults with the following national breakdown: Canada, 1000; India, 2000; Indonesia, 500; Malaysia, 500; Philippines, 500; Singapore, 500; UAE, 1000; UK, 1000; USA, 2000.

Forrester data

Callsign commissioned Forrester Consulting to conduct a survey of senior decision-makers from financial organizations across the globe.. 40% were from North America, 20% were from the UK, 20% were from APAC, 19% were from the Middle East.



callsign[®]

Balancing security, UX & privacy is easier than you think.
Find out how we can help you on your journey to
digital leadership – callsign.com.

Get in touch for a demo of our
capabilities: sales@callsign.com

© 2023 Callsign Inc. All rights reserved.