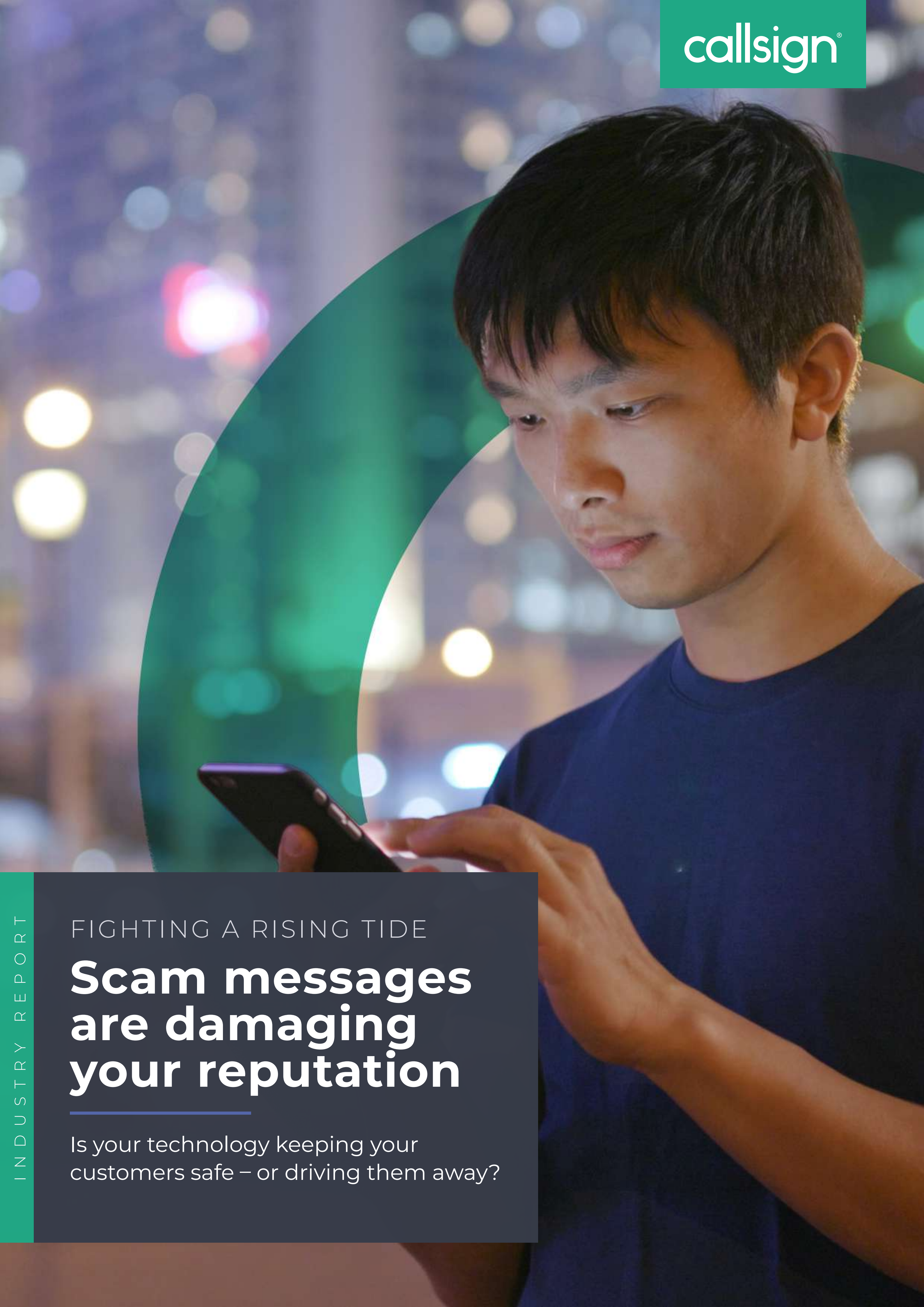


INDUSTRY REPORT

FIGHTING A RISING TIDE

Scam messages are damaging your reputation

Is your technology keeping your customers safe – or driving them away?

This report will explain the critical steps that every business should be considering:

1. Moving away from a reliance on SMS for authentication to more secure methods such as in-app
2. Communicating that move to customers
3. Assuring them that you won't contact them via SMS or email and ask them for any personal data
4. Considering the use of dynamic interventions to help steer customers to safety when they do fall for online scams

AN UNCHECKED PROBLEM

Your reputation is at risk

That's an unwelcome message, but it's one that needs to be heeded and, more importantly, addressed. And coincidentally, that's a pointer to the source of the danger: unwelcome messages.

We've all been there. In a café, at home on the sofa, on public transport – that telltale ping on our phone that indicates yet one more scam message.

On average, consumers receive 1133 scam messages a year; that's the equivalent of 3 a day. And some of those messages are very convincing indeed. It's a certainty that we all know someone who, if not caught out by a fraudulent message, has at least had a close shave.

For customers, those messages elicit a variety of reactions, even if they manage to avoid being taken in by the scam. Anger, frustration, anxiety – these are all common and understandable emotional responses to scam messages. All of which, as these findings show, are directed towards whichever organization the scammer is masquerading as. The result is – for a huge 45% of people – a loss of trust in that business.

If that organization is yours, then you have a serious problem on your hands.

Customers expect the businesses that they deal with to protect them and keep them, their data and their finances safe. And if you're authenticating customers in the same channels that the bad actors are using, then you're not doing that.

45% of consumers lose trust in your organization if it's named in a scam message

The scale is global

Underestimated, under-reported and largely unchecked: fraud is a problem of global proportions and one that's on the rise with no sense of slowing.

Globally, 98% of people have received a fraudulent or scam message on one or more channels in the last year; that's the equivalent of 21 messages per week, every week, for every person.

And a high percentage of those messages are finding their mark. Across the world, from Houston to Cape Town to Singapore, 44% of people have been victims of fraud.

The many faces of fraud

The actual communication channels are only one part of the story, albeit an important one. A more immediate concern is where these messages (seemingly) originate from.

With money being the primary driver for the vast majority of fraud, it's hardly surprising that the vast majority of scam messages – 59% of people have encountered messages masquerading as genuine communications from banks and financial institutions.

E-commerce and retail is, unsurprisingly, not far behind. With online now the main channel for many consumers, bad actors are also making tangible efforts in that arena, with over a third of people receiving messages claiming to represent one of these types of businesses.

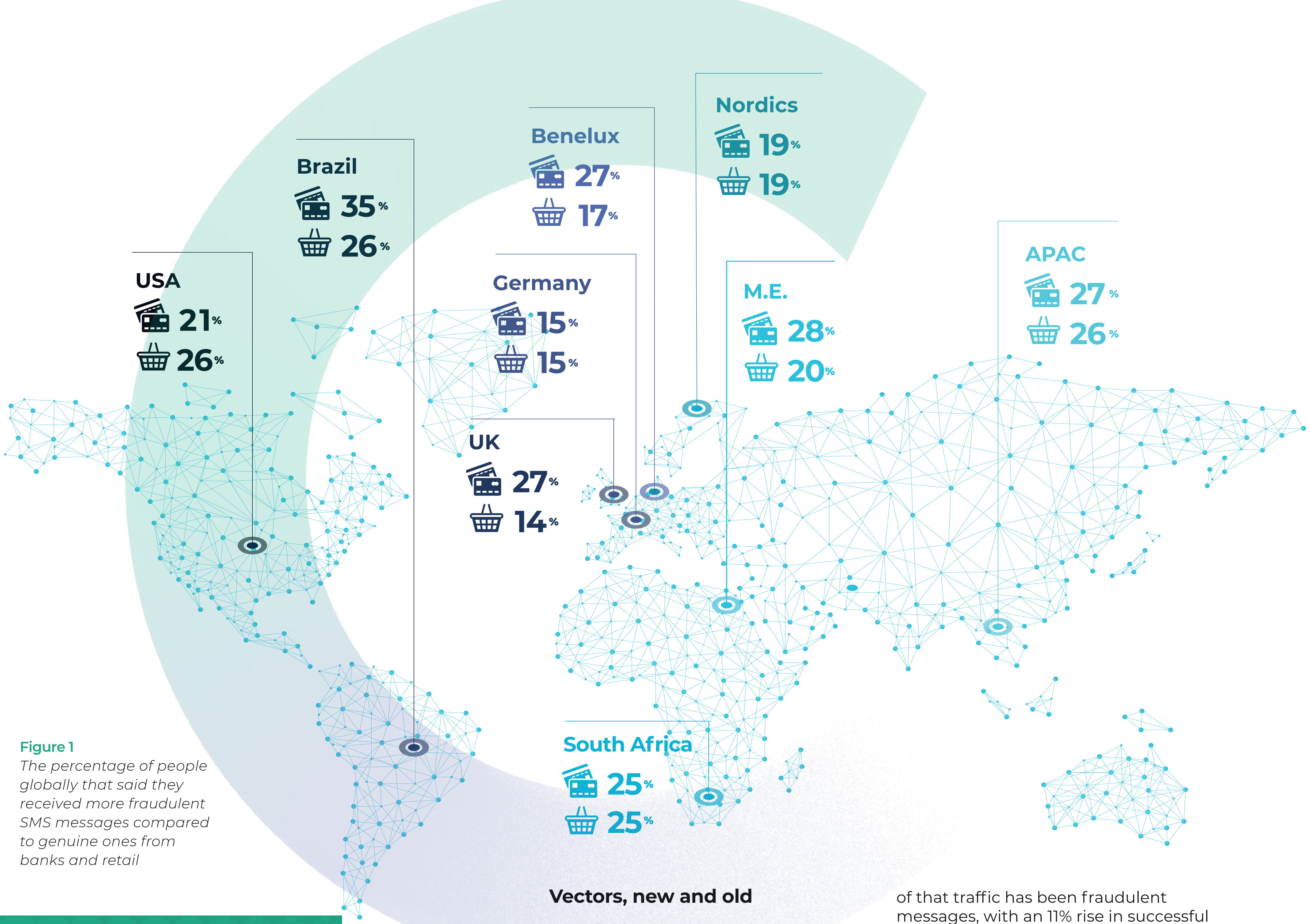


Figure 1
The percentage of people globally that said they received more fraudulent SMS messages compared to genuine ones from banks and retail

98%

Globally, 98% of people have received a fraudulent or scam message on one or more channels in the last year...

21

that's the equivalent of 21 messages per week, every week, for every person.

Vectors, new and old

Whilst email & telephone continue to be the common channels targeted by scammers, they're not the only ones. SMS text messages, social media and messaging apps are increasingly being used as attack vectors by fraudsters; all of which adds to the volume that we receive on a daily basis.

Once again, the numbers related to the proliferation for these channels are deeply concerning. Text messaging, which was declining rapidly to the point at which it was predicted that it would disappear altogether, has surged in the last few years; a significant portion of that traffic has been fraudulent messages, with an 11% rise in successful SMS-related fraud in the last year alone.

As for email – **in the UAE, people are more likely to receive an email from a fraudster than they are from a member of their family.** And the rest of the world isn't far behind.

Other channels have seen similar patterns of growth, and the direct result of this is that **people's overall trust in all of these channels has decreased. For SMS, that trust has dropped for 55% of the population**; for social media companies, it's even higher at 59%.

CUSTOMER PAIN POINTS

So, the scale of the problem is clear. Or is it?

As worrying as those numbers are, the reality is likely to be much higher. Only half of the survey respondents who had received a scam message had reported it – to their bank, to the retailer, to the police, to anyone.

Those frustrations are not being helped by the lack of clarity around exactly what the recipient of such a message should do about it. Of the 50% who didn't report the messages, 37% simply didn't know who to report it to. Here, one of the complicating factors is the wide range of organizations that scams can seemingly originate from; and more than one could be referenced in a message.

And with the high volume of scam messages being received, almost the same amount of people felt that they got too many messages to even bother. And tellingly, 16% felt that reporting messages was a pointless exercise, and that the bank or retailer wouldn't be able to do anything about it.

WHERE DO CONSUMERS REPORT FRAUD?

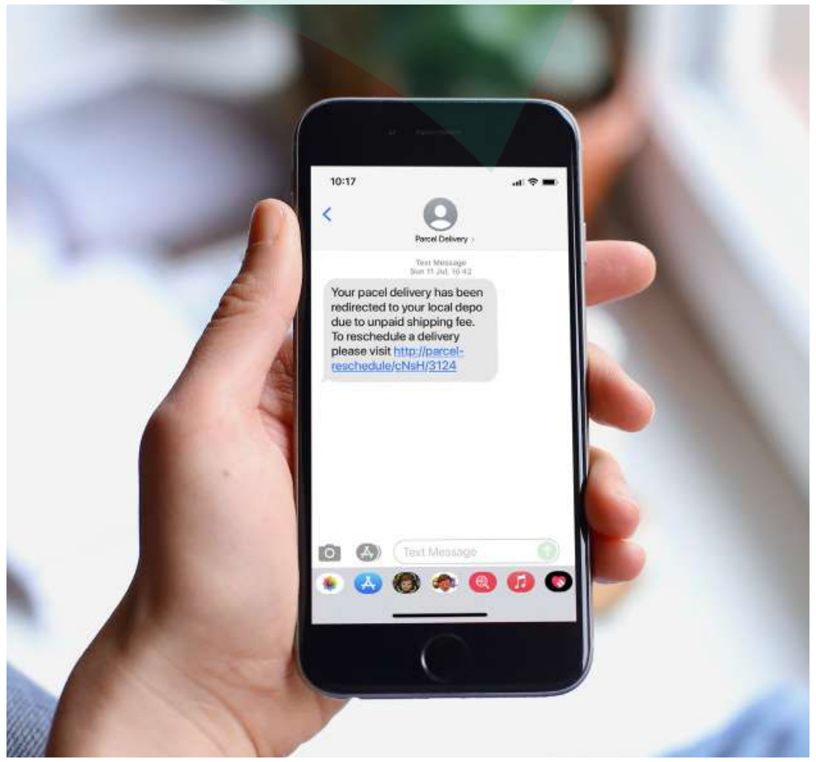
24% BANKS

21% MOBILE NETWORK PROVIDERS

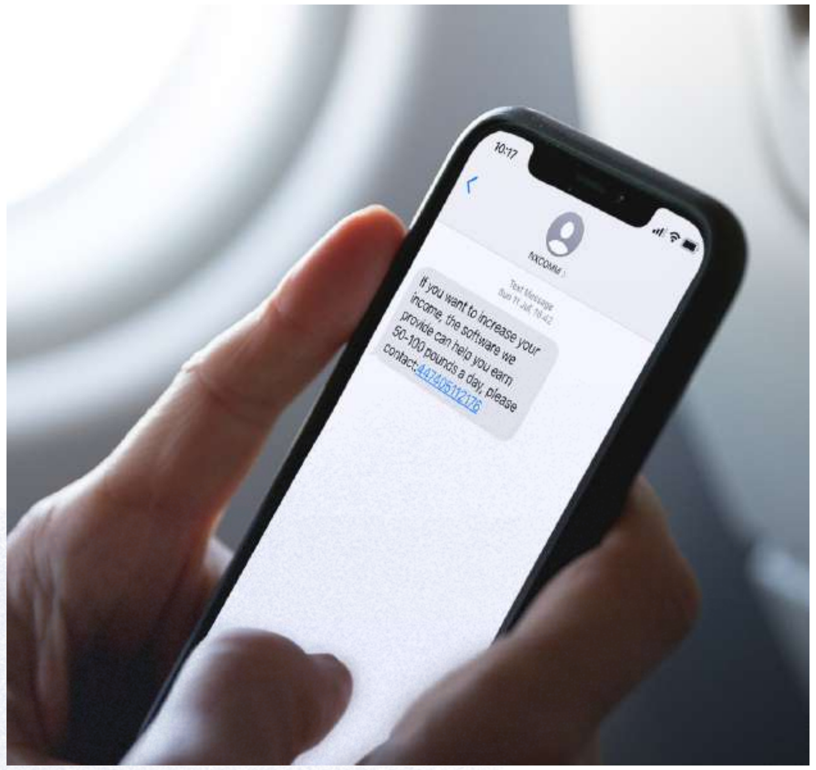
12% RETAILERS

11% CRIME AUTHORITIES

9% THE POLICE



Your pacel delivery has been redirected to your local depo due to unpaid shipping fee. To reschedule a delivery please visit http://parcel-reschedule/cNsH/3124



If you want to increase your income, the software we provide can help you earn 50-100 pounds a day, please contact:447405112176

Hard to spot

The blockers in and around reporting scams are exacerbated by the fact that a great many scams are extremely hard to spot. Many people have something of a blind spot when it comes to scams; It's all too easy to be lulled into a false sense of security and to believe that you won't be caught out.

But people still get caught out, every minute of every day. It's disingenuous to blame the customers; bad actors can and will use every tool and technique at their disposal to conduct their shady business.

Their approaches can range from the tried-and-tested arsenal of bots, malware and Remote Access Trojans (RATs) that are only getting more sophisticated. Equally sophisticated are the 'off-the-shelf' software kits that can emulate login portals with a high degree of accuracy.

And scammers are becoming increasingly adept at social engineering approaches, convincingly masquerading as genuine agents from legitimate organizations – and using their knowledge of an organization's user journeys to coach and coerce their victims into bypassing the static warning messages that businesses all too often rely on.

It's getting personal

It's a reminder that fraud is emphatically not a victimless crime. For the consumers who are snared by fraud, the impact is considerable – and not simply from a financial perspective. While this can be significant, it's important not to underestimate the psychological implications that go hand in hand with fraud.

Embarrassment, shame and even fear all play their roles in keeping scams unreported. Over a fifth of people said that they'd felt vulnerable after receiving a message; more than a third expressed anger.

What becomes troubling for organizations who are namechecked in a scam is the impact on consumers' perceptions the receipt of these messages. 38% had concerns about invasion of privacy; 43% raised questions around how said scammers got their information in the first place. Consumers are increasingly aware of the value of their data: high. So it's no wonder that **almost half of consumers are not comfortable sharing personal data with *any* organization**.

And the same number of consumers will only stick with an organization that they aren't comfortable sharing their data with because there's no alternative.

The (high) value of choice

That alone should be a wake-up call for any organization to up its game. Customers who are on the verge of churning are more likely to simply jump ship than flag their concerns.

From the customer viewpoint, choice is important – really important. Shopping around for the best deals is second nature to consumers and with online the first choice for more and more people, it's never been easier to do so.

Percentage of people who were uncomfortable sharing their data with organizations

28%	BANKS
41%	RETAILERS
47%	ONLINE PLATFORMS

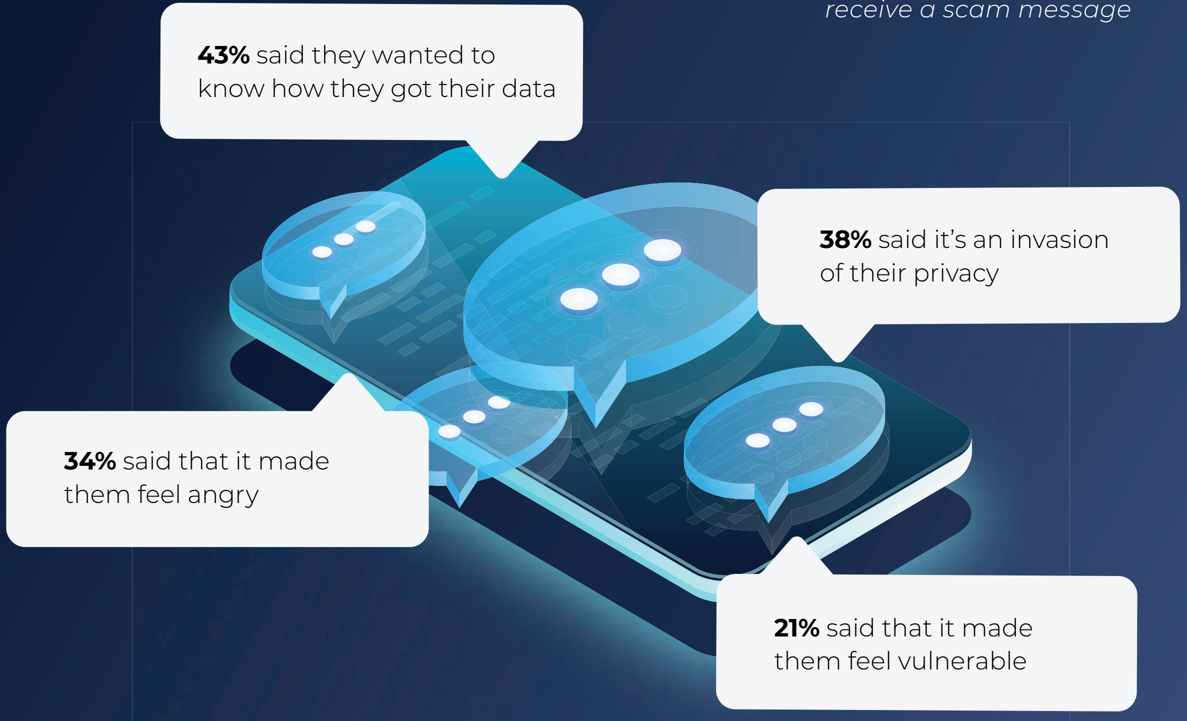


Figure 2
How customers feel when they receive a scam message

43% said they wanted to know how they got their data

38% said it's an invasion of their privacy

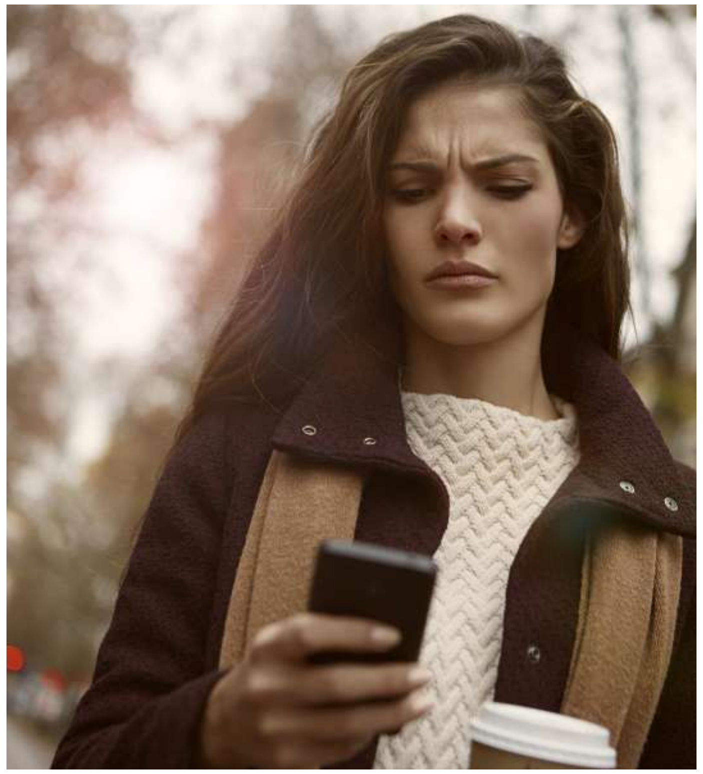
34% said that it made them feel angry

21% said that it made them feel vulnerable

And if something about the service they're receiving upsets them – such as being scammed – **that's exactly what they'll do, with the majority opting to stop using the company whose name the fraudster used rather than changing communication providers.**

Responses and responsibility

When it comes to scam messages, your actual business might be a contributing factor. 88% of respondents feel that the responsibility for preventing those scam messages lies with the bank or the company whose name the fraudster used, or the organization operating the channel through which it was delivered: email and messaging app providers, or mobile network operators and social media companies.



UNCHANGED BEHAVIORS

Only 33% of people feel that it's difficult to tell if a scam message is genuine; but the 64% who do might well be overestimating their own abilities. Big time.

And what's interesting is what many people do after being caught out: nothing.

Why is this the status quo? That conundrum (and the behavioral psychology behind scams) is explored in our whitepaper, **Wild, Wild Web**. Combining original research with insights from leading behavioral scientists, it's invaluable reading for any business seeking to protect and educate its customers.

UNDERSTANDING THE BUSINESS IMPACT

The digital trust dividend

The belief that organizations should be more accountable for the situation goes well beyond responsibilities,and it's something that all businesses should be taking note of:

Block

21% of scam victims will stop using the business that was named in the scam message

The impact that scams is having on businesses globally is stretching far beyond the risk of fraud itself. By proxy, we're all responsible – whether we like it or not.

Trust: hard won, easily lost

Of those who have been scammed, a quarter blame the company named in the message and the consequences of that isn't good: **over a fifth (21%) stopped using the company whose name |the fraudster used and 32% trust that company less**. That might seem harsh; the company in question could argue that it had nothing to do with the fraud.

But only at first sight. When we unpick the reasons for this lack of trust, a picture starts to emerge. Almost half of consumers (46%) felt that the organization isn't capable of keeping their personal information secure, and a fifth stated that the company couldn't certify their identity.

Time to change the channel?

When we ask respondents about the channels they're using, the picture as to why they're blaming your business over the fraudsters becomes clearer. Whilst many seem comfortable using more common channels to communicate, the newer digital channels are proving to be gaining traction with 31% opting for in-app.

However, when it comes to which channels consumers perceive to be safe the tables really do turn. When it comes to building digital trust, it's key that the avenues that are used to communicate with customers are safe and easy to use.

At the moment we're relying on the same channels to authenticate consumers as the fraudsters are using to scam them. It's no wonder trust is eroding from all angles and that only 5% of global consumers think SMS is a safe way to communicate.

Reenforcing the foundations of identity

For businesses, this is where the most severe impact makes its presence felt. Digital trust is foundational, probably the most important factor for any business as we increasingly interact online. And digital identity is the foundation that underpins this trust, sitting at the core of every digital interaction. And right now, if we're not getting this right, that's a bit of a problem.

The way things stand, customer loyalty has never been more fragile. Acquiring and keeping customers is not an easy or cheap process, and all of that work can be undone by a single fraud message.

It's an indicator of the tenuous nature of digital trust. If a single text message is all it takes to shatter a customer's trust in a business, then it's clear that digital trust is very badly broken indeed.

Which of these channels do you think is the safest to communicate with your bank or retailer?

32% IN-APP

31% TELEPHONE

17% EMAIL

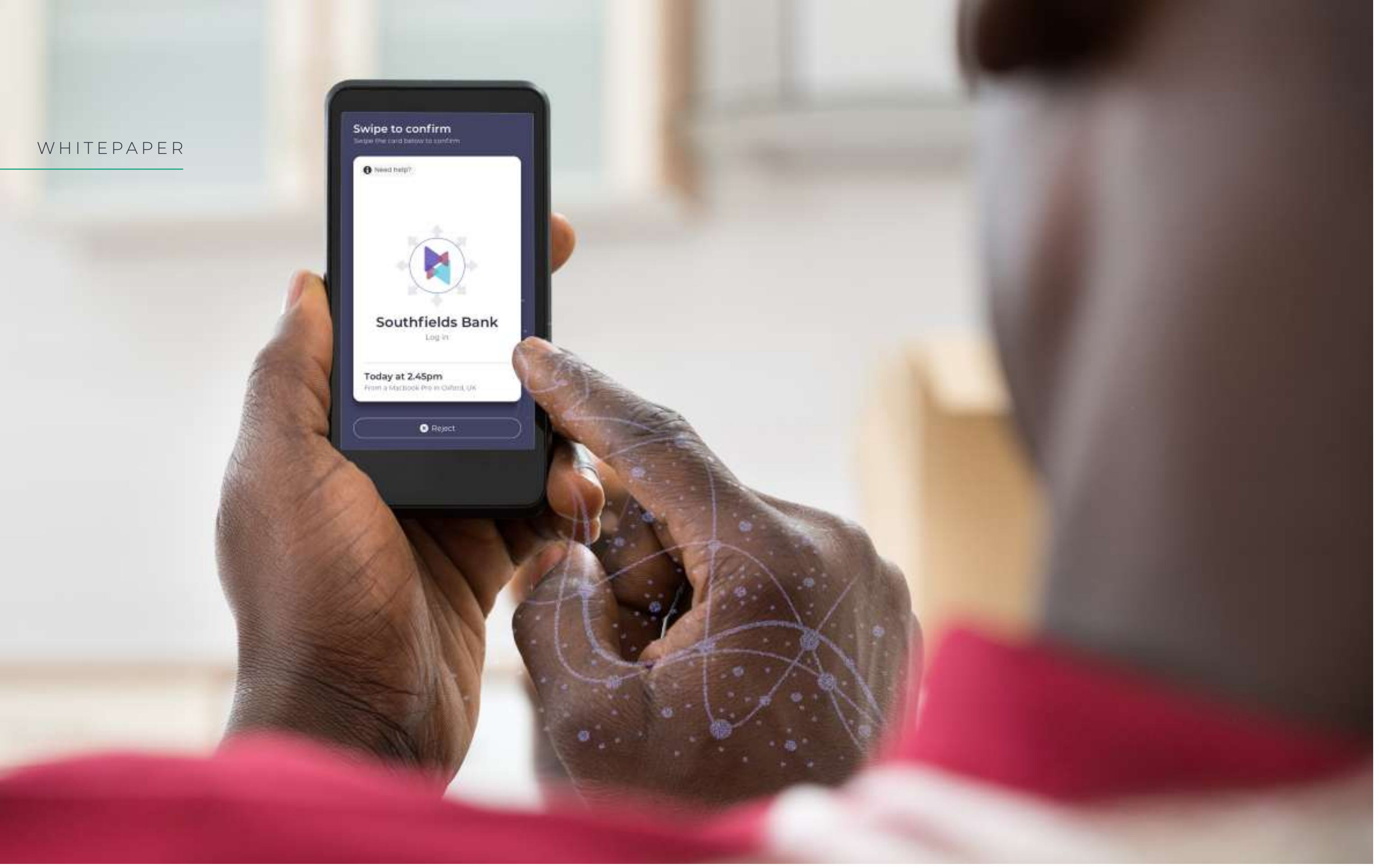
5% TEXT MESSAGES

4% SOCIAL MEDIA

2% CHAT BOTS

ONLY 5%

Only 5% of consumers feel that SMS is a safe way to communicate with your company.



POSITIVE IDENTIFICATION

A digital solution for a digital world

The outlook isn't as bleak as it might seem, however.

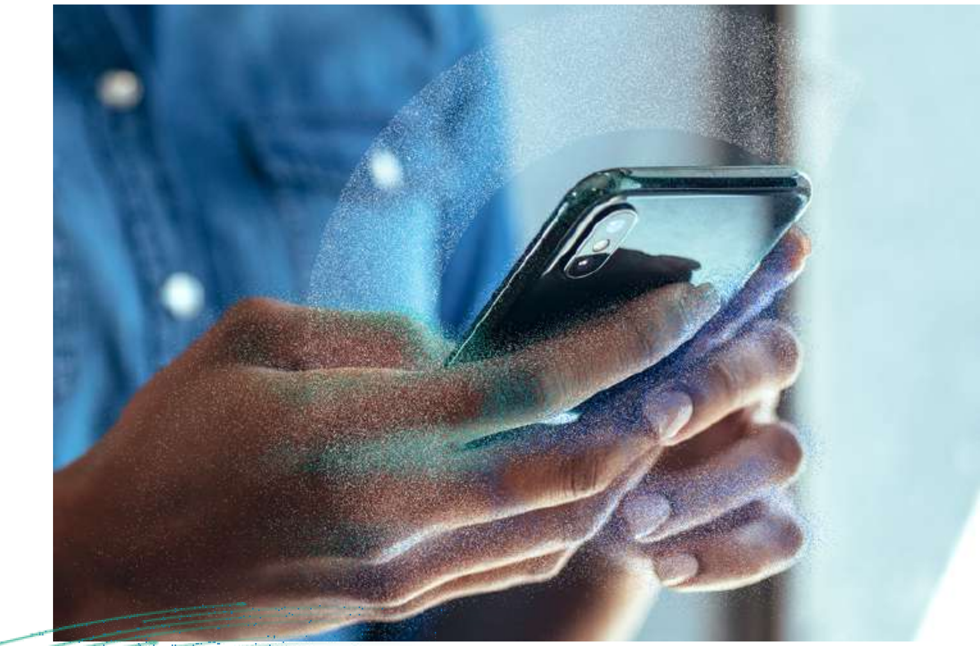
The bad actors – the fraudsters, scammers and cyber-criminals – who are driving the numbers upwards – are not infallible. When they encounter authentication mechanisms and scam prevention technologies that they can't circumvent, they'll quickly give up and move onto softer targets.

And it's technologies such as Callsign's next-generation behavioral biometrics, that present any would-be fraudster with these impossible tasks.

Because behavioral biometrics are keyed to the unique inherence factors of each user – the way they tap, type or swipe, even the way they hold their device – the most dedicated bad actor will give up long before they get anywhere near gaining access.

And behavioral biometrics are just one of the technologies that make up Callsign's watertight authentication and fraud prevention solution. Our AI-driven ensembling uses machine learning to passively recognize a legitimate user, even if they're using a different device or in a different location by passively analyzing thousands of data points across device, location, behavior and any third-party systems.

Callsign can protect your customers even in situations where bad actors are employing social engineering tactics. Rather than rely on static warning messages that scammers can predict and talk their victims around, our Dynamic Intervention solution can recognize the unusual behaviors that indicate a fraud in progress – such as attempting to make a large money transfer whilst typing one handed – and prompt the user with a customized warning message that the fraudster will be unable to anticipate or talk their way around.



Joined-up assurance

Put it all together – which is simplicity itself with our Orchestration Layer, which allows our technologies to seamlessly interact with any existing or legacy systems – and it all adds up to a watertight solution that lays out the red carpet for legitimate customers and bars the door against the fraudsters.

Right at the very start, we said that fraud is a problem that's largely unchecked; and the operative word in that sentence is *largely*.

Callsign's technologies represent a major step forward in taking the fight back to the fraudsters, and keeping your customers and their data safe and secure.

callsign®

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

Or get in touch for a demo of our capabilities: **sales@callsign.com**