FACES OF FRAUD

Consumer experiences with fraud and what it means for businesses

sas

contents

Executive summary

As explored in a new study commissioned by SAS, there's almost no area of people's lives that can't be exploited by fraudsters in our increasingly connected world. Perpetrators can gather information, target tens of thousands of unsuspecting consumers online via text messages, phone calls and social media, and use that information against them in increasingly insidious ways.

Concerns about fraud are growing among consumers – and our findings, which are based on surveys of 13,500 people from around the world, indicate that a high proportion of them have already been targeted.

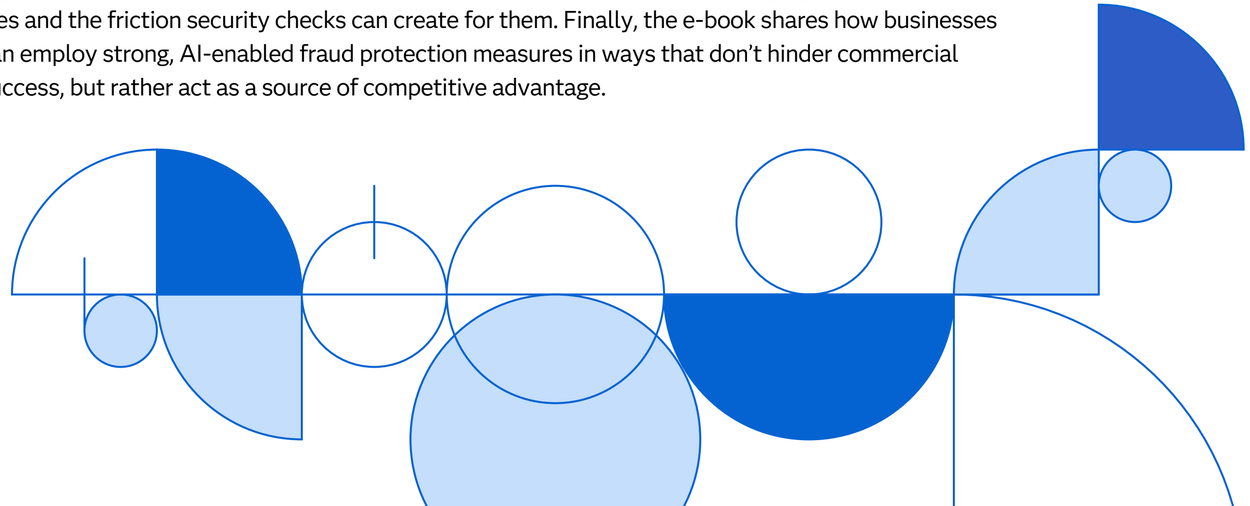
The study also highlighted global trends in consumer-focused fraud. For example, fraudsters are increasingly masquerading as energy firms, couriers, banks, lottery companies and even romantic partners, operating at scale to extract money, sensitive information or both from their unsuspecting victims. Often, they succeed by using emotional manipulation or by simply catching people off their guard.

Fraud against consumers soared during COVID-19 as scammers exploited the shift to online work and shopping and growing personal financial crises. Some impersonated utilities and government agencies by offering food, financial assistance and medical supplies for payment; others took advantage of feelings of loneliness created by the lockdowns by engaging in romance scams. In some areas of the world, higher demand for dogs during the pandemic even led to a rise in "pet fraud," where scammers target people with cute photos of animals to hook potential "buyers" and use false stories to lure them into sending money.

At the same time, inflation has made investing more attractive to savers, thus exposing them to new types of fraud. Consumers in the US, for example, reported losing more money to investment scams than any other category – almost $3.8 billion in 2022, twice as much as in 2021. In addition, buyers in the unregulated crypto market appear particularly vulnerable to fraud. Following the collapse of FTX at the end of 2022, there were fears that fraudsters would "exploit uncertainty and target those trying to recover lost investments through fake exchanges and scams involving initial coin offerings." There have also been reports around the world of scams ramping up around tax deadlines, as well as fraudsters targeting job seekers by enticing people with tempting offers of remote work.

Clearly, everyone has a role to play in fighting fraud, from everyday citizens and governments to law enforcement agencies responsible for educating the public and securing convictions of wrongdoers. But what do these trends mean for businesses, particularly those in the financial services, telecommunications and insurance industries that, as explored in this paper, may be unwittingly acting as conduits for criminal activity?

This e-book explores fraud trends in more depth and their implications for consumers and businesses. It delves into study findings that shed light on the changing expectations consumers have for the organizations they work with, as well as new consumer attitudes about emerging security technologies and the friction security checks can create for them. Finally, the e-book shares how businesses can employ strong, AI-enabled fraud protection measures in ways that don't hinder commercial success, but rather act as a source of competitive advantage.



About the study

At the end of 2022, SAS commissioned 3Gem Research and Insights to undertake a global study into some of the key trends in fraud against consumers. The findings are based on a sample size of 13,500, with a 50/50 split of men and women. As shown in Figure 1, this study spanned the US and Canada, the EU, the UAE, Brazil, South Africa and beyond.

For more details about the participants in the study, see Appendix A.

13,500
Consumers surveyed

16
Countries represented

4
Continents represented

18 and up
Age range of participants

Global findings

Concern around fraud is growing – but are consumers more savvy?

Almost half (47%) of the consumers surveyed say they experienced more fraud in 2022, even as the pandemic subsided in many parts of the world. However, the figures are notably higher in some countries than others. South Africa topped the list at 65%, followed by Portugal at 62%. At the other end of the scale, in the Netherlands, the proportion grew by a more modest 32%.

Looking beyond 2022, more than 70% of those surveyed said they have been the victim of fraud at least once during their lifetime. Approximately 17% reported falling prey to fraud several times.

Given the pervasiveness of fraud today – and the range of financial loss and trauma victims can suffer – it's no surprise that three-quarters of those participating in the survey said they are fearful of becoming a victim. The pervasiveness of this fear varies by country, however. In Brazil, for example, 94% of those surveyed are afraid of falling prey to fraud, and in the UAE, 83% report significant levels of fear. In contrast, only around half (53%) of consumers in the Netherlands express concern.

Just over 70% of those surveyed said they have been the victim of fraud at least once during their lifetime. Approximately 17% reported falling prey to fraud several times.

Approximately 86% of all consumers surveyed globally reported being more wary of fraud now – at the time of the survey – than they used to be, and nearly half (46%) are "significantly more" so than in the past. This is likely due to a combination of:

- Increased news reports.
- Growing warnings by government and industry regulators regarding consumer fraud.
- Recent economic crises.
- Growing consumer reliance on online channels, which require them to share more information digitally, create and manage passwords and make online payments.

Concern about fraud is leading to more protective actions, however. Asked how they would respond if they were contacted by someone they weren't expecting, 98% of those surveyed said they would either ignore it or try to establish whether the person was legitimate.

Even so, when fraudsters are convincing, it's easy for even savvy consumers to be caught off-guard. Less than half (43%) of those surveyed said they would try to establish whether a contact was a legitimate inquiry – which means they run the risk of revealing information that could be of value to the fraudster.

Who's most at risk?

Anyone can be the victim of a fraud, especially if criminals strike at the right time. For example, when someone is awaiting the delivery of a parcel from a legitimate courier, they are vulnerable to an email or phone scam from someone masquerading as the shipper. But certain groups of people are at higher risk than others. For example:

- Gen Z consumers in the US (born 1997-2012) who grew up with the internet are more likely to be a victim compared to millennials and Gen Xers. Fraudsters know how to effectively target them via social media.
- Younger people in the EU, and those who have a higher level of education, are also susceptible because they shop online more. Yet in the UK, this group is the least likely to be a fraud victim – just ahead of the over-75s, who may be less vulnerable because they typically spend less time online.
- Disabled adults are at higher risk than non-disabled ones, and renters are more likely to be a victim than homeowners.

Types of fraud

Where are the vulnerabilities?

Identifying and preventing fraud has always been a challenge, because bad actors continuously adapt their strategies as detection methods improve and digital technologies evolve.

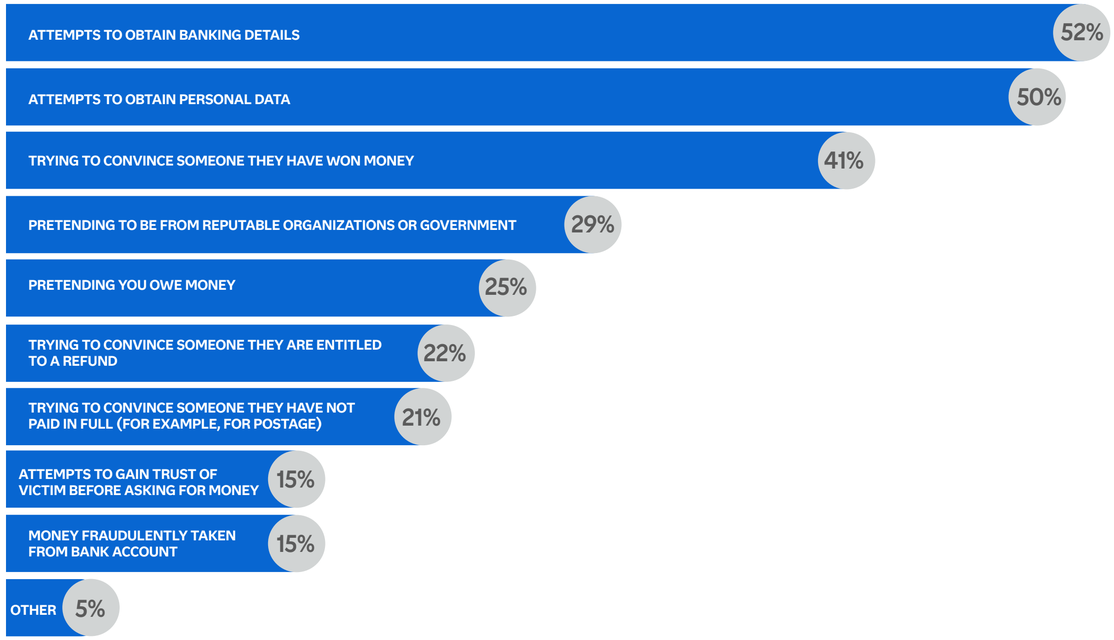
This was particularly apparent during – and after – the pandemic. In the immediate wake of the COVID-19 pandemic, the digital economy exploded. For fraudsters, the sudden surge in digital transactions and payment modalities offered countless new avenues for fraud. Scammers largely focused on pandemic-themed schemes and socially engineered attacks.

But the landscape has changed. By 2023, it was clear that the digital economy and the "global scam economy," as described in a recent global report by Javelin, are here to stay – and they will evolve in parallel. Previous pandemic-focused schemes have been replaced by new scams such as romance scams, fake home-based employment opportunities and investment schemes.

As summarized in Figure 2, the study highlighted at least nine types of fraud being perpetrated today. All nine are driven by either a financial motive or an attempt to acquire personal data. Fraudsters trying to obtain bank details accounted for just over 50% of fraud cases, followed by attempts to steal personal data. Competition scams such as lotteries – which are easy to promote online and tempting to many people – were the third most common type of fraud, according to the study. These scams are usually attempts to harvest personal data or infect a computer with malware.

The vast majority of fraud cases involved some kind of deception. Deceptions uncovered in the study ranged from simple yet convincing phishing emails where the victim inadvertently clicks on a link, to cases where the victim is befriended or enters into a relationship with the perpetrator and is persuaded to part with their money or personal information.

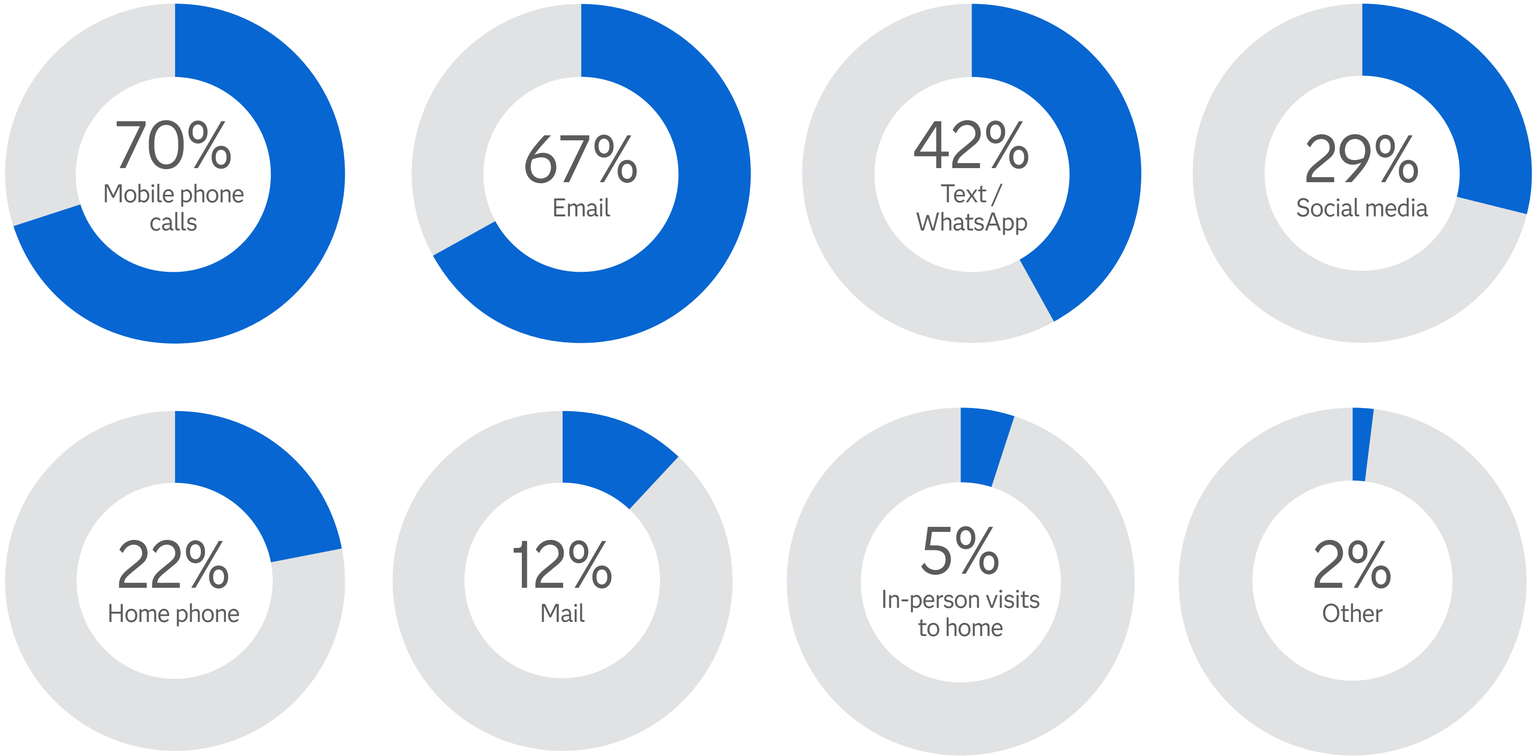
Figure 2: *Most common types of fraud strategies*



As shown in Figure 3, the study also revealed the most common communications channels fraudsters use. Mobile phone calls top the list. It's important to point out that these "fraud calls" don't include unsolicited sales calls where consumers are persuaded to buy what might be a substandard product or service. Rather, phone call-based fraud refers to scams where the primary goal is to extract inappropriate payments and/or personal data from unsuspecting consumers.

Some scams involve automated calls that target thousands of users at once, or as the UK's National Cyber Security Centre points out, use information about a consumer that they find online to sound more convincing and build trust. Scam calls can also involve a perpetrator pretending they are from a trusted organization, such as a government agency.

Figure 3: *Common communications channels used by fraudsters*



Could consumers spot these types of fraud?

1. Buy now, pay later (BNPL) fraud

The use of BNPL soared during the cost-of-living crisis, according to Forbes. But while it offers a convenient and flexible payment option and is popular among younger people, fraudsters can take over or open accounts using a victim's details, running up huge bills and charges and damaging credit scores due to missed payments.

2. Account takeover fraud

With people living so much of their lives online today, especially since the pandemic, account takeover fraud has become even more lucrative for criminals. Typically, they buy details on the dark web or extract them from victims through deception to take over shopping or banking accounts. The availability of generative AI tools makes it easier to create deepfake profiles.

3. Credit card fraud

The chips in credit cards today make it more difficult to clone them and commit fraud at checkout points compared to those with a magnetic stripe. Now the risk associated with credit cards has shifted online, with fraudsters making purchases using a card and its associated CVV number. In the US alone, card-not-present fraud is expected to account for almost three-quarters of payment card fraud, with losses totaling $9.49 billion.

There have also been cases of fraudsters using WiFi networks to install malware on PoS (point-of-sale) devices to disrupt transactions. These disruptions force consumers to type in their PIN. Then, when the card is inserted, both the chip and PIN are copied by the malware.

4. Lottery fraud

News that someone has won a substantial sum of money can lead them to handing over sensitive information, such as their name and bank details, without questioning the veracity of the award or the trustworthiness of the person making the claim. In other cases, consumers lose money by calling premium-rate numbers (telephone numbers that charge higher price rates for select services) to claim a prize that doesn't exist.

5. Romance

In the age of social media and online dating apps, it's easier than ever for fraudsters to pose as a potential love interest. The US Federal Trade Commission points to three common behaviors that romance scammers display: they make up excuses about why they don't want to meet up in person, they request money, and they tell the victim how to pay (such as an international money transfer service Western Union or gift cards). Romance scams may be under-reported, as victims often feel ashamed of having been deceived and defrauded.

Protecting consumers

Who's responsible?

While many types of fraud rely on consumers voluntarily sharing information or making payments, there are other ways it can materialize. Sometimes, they might feel compelled to take actions that lead to suffering or loss. For example, in WhatsApp fraud or Messenger fraud, a perpetrator exploits social media content to pose as a family member facing some type of risk in order to extract data and money from another family member. In other cases, flaws in online security, such as not including two-factor authentication into the design of a corporate website (so customers can choose to bolster their security), may make it easier for scammers to complete fraudulent transactions.

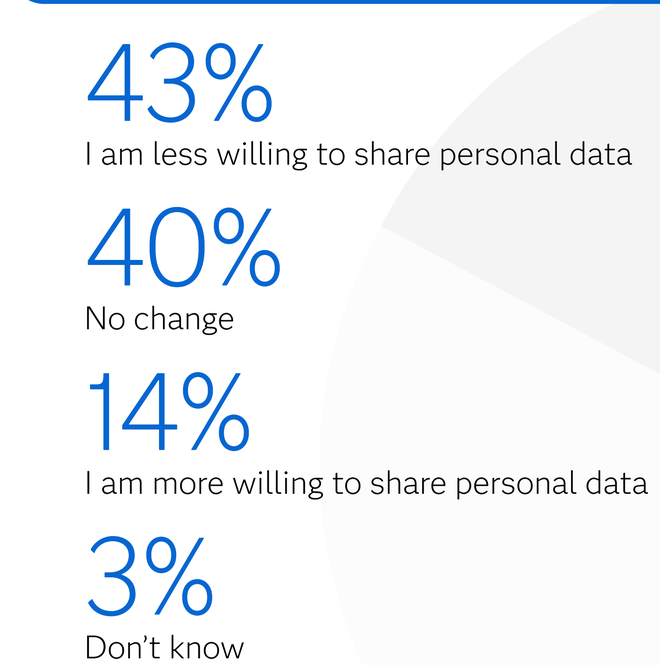
Financial services is the industry fraudsters are most likely to target, but fraud is a major threat to other industries such as telecommunications. For example, fraudsters can abuse corporate networks by executing large volumes of automated voice calls (an attack referred to as vishing) and text messages, including ones to premium rate international numbers. Similarly, email providers and social media platforms can be exploited to send messages that appear genuine, but they are actually an attempt to target unsuspecting consumers at scale.

For this reason, companies have a responsibility to identify and act on reports of suspected fraud. Ultimately, consumers want to feel that their personal information is safe and secure, as our study made clear. Globally, 89% of consumers surveyed believe that the organizations they engage with should be doing more to protect people from fraud; the numbers are even higher in Brazil (98%) and South Africa (96%).

There's also a significant commercial incentive for businesses to invest in fraud detection and prevention initiatives. Globally, 67% of those consumers surveyed said they would switch to another provider if they experienced fraud or felt that another company offered better protection. This proportion was much higher in some countries such as South Africa (88%), Brazil (84%) and Spain (76%).

Consumers also have a role to play in protecting themselves. Their growing awareness of the risks of fraud may also be the reason why 43% those surveyed across all countries said they are more cautious about sharing personal data with companies today (at the time of the survey) compared to the past (see Figure 4).

Figure 4: *Consumer willingness to share personal data*



Most of those surveyed, however, report that they are still comfortable using digital services, rather than interacting on the phone or in-store, and they don't plan on changing their behavior (see Figure 5).

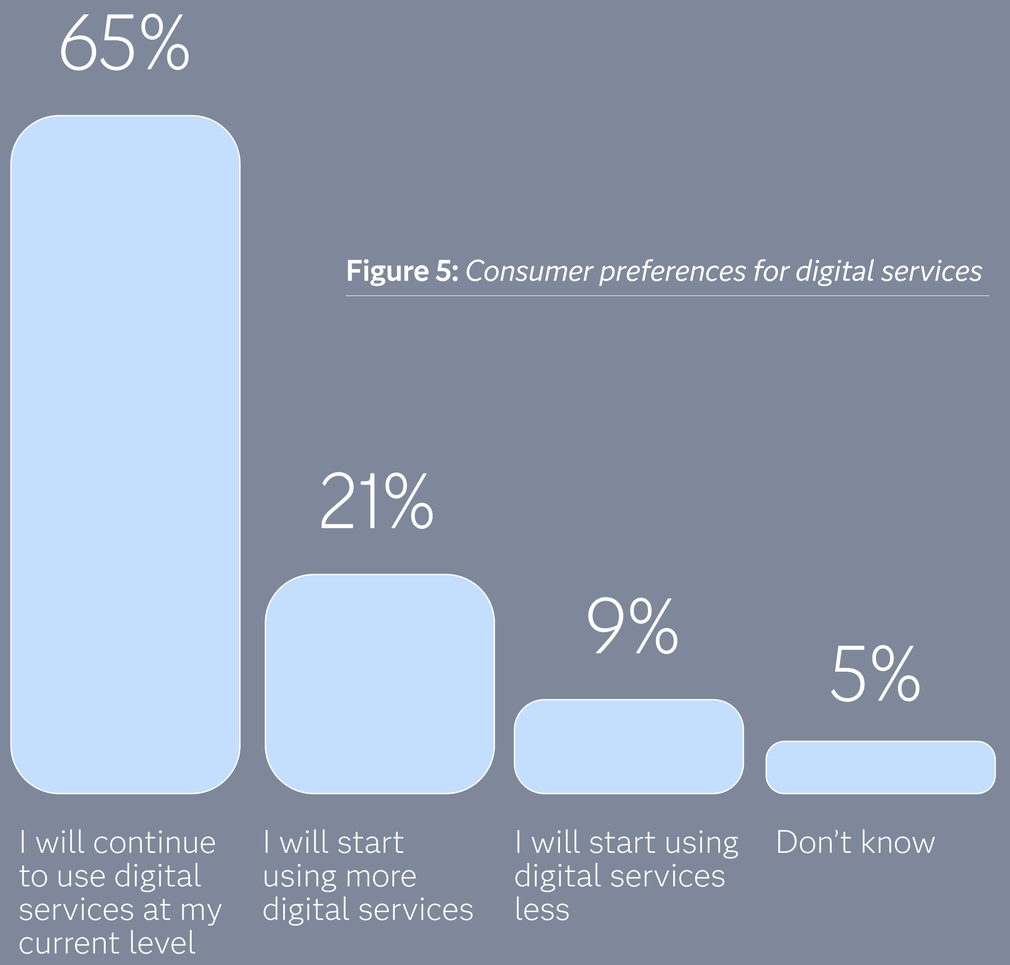
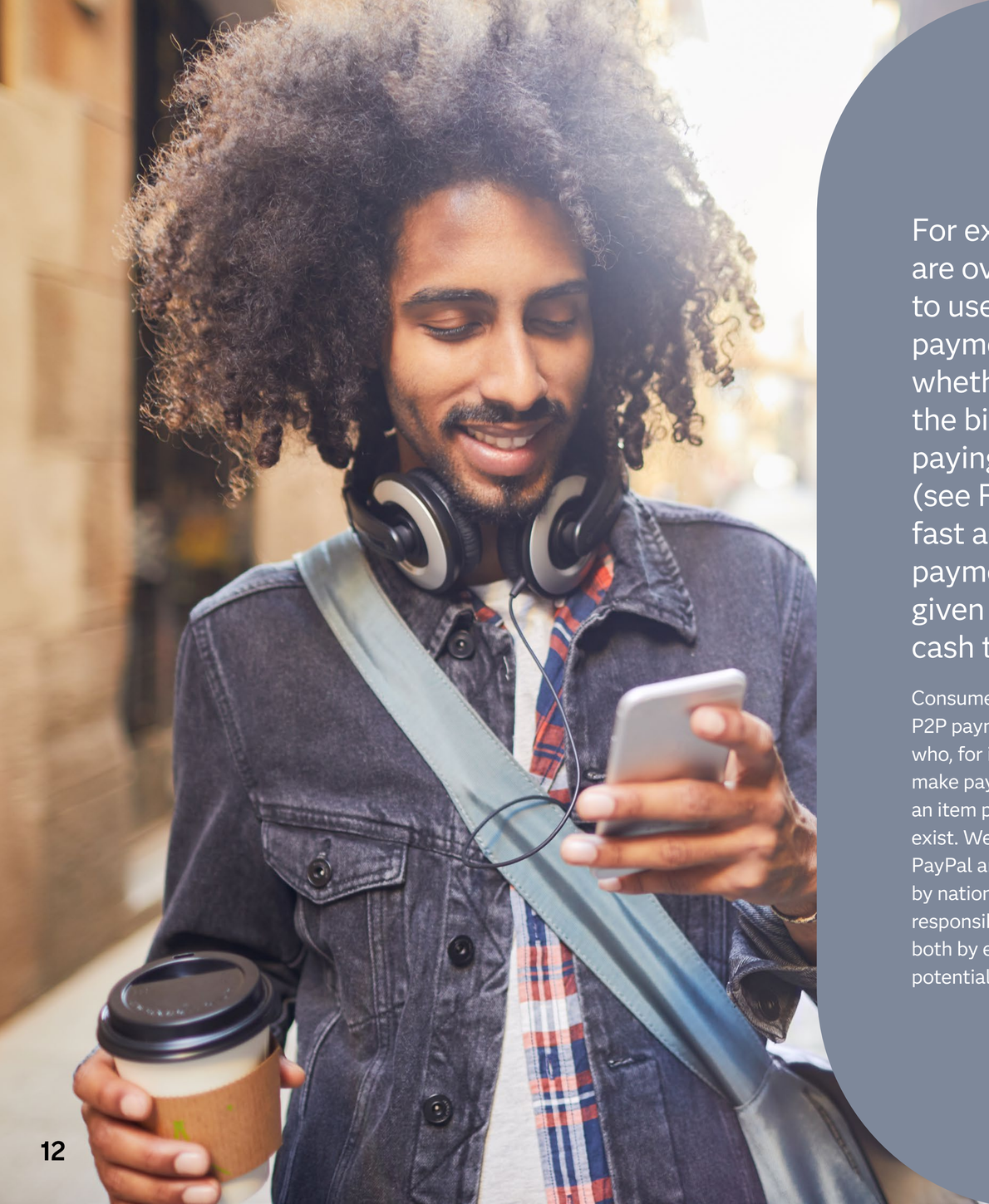


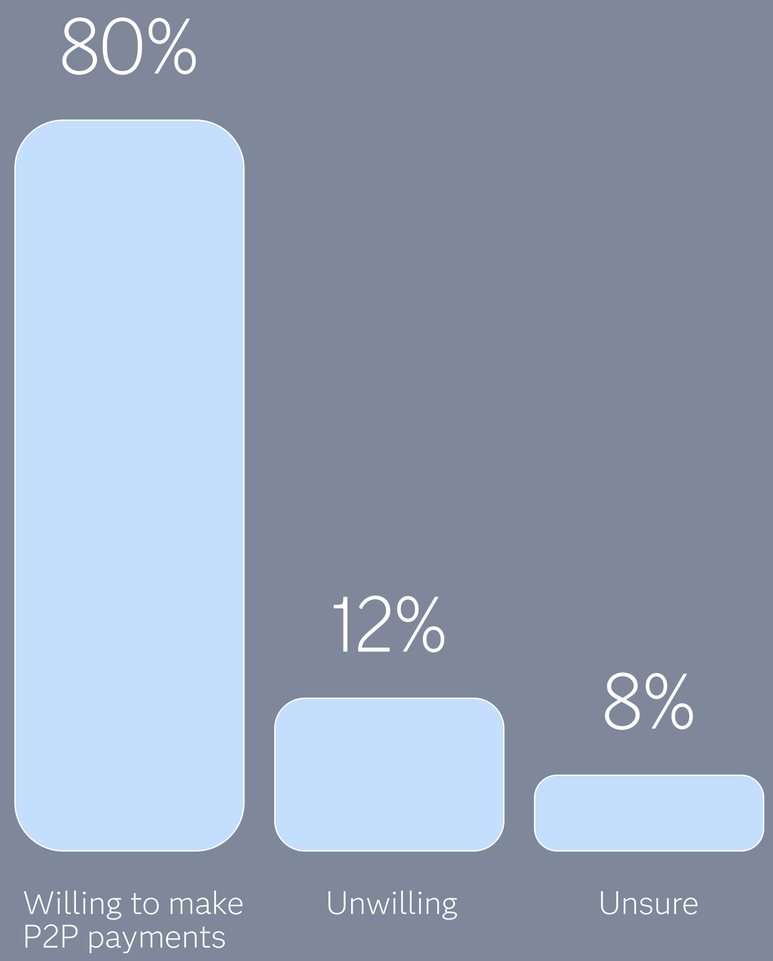
Figure 5: *Consumer preferences for digital services*



For example, consumers are overwhelmingly willing to use peer-to-peer (P2P) payments to pay individuals, whether with friends splitting the bill at a restaurant or paying rent to a landlord (see Figure 6). This can be a fast and convenient digital payment method, especially given that fewer people carry cash today.

Consumers are often unaware how easily P2P payments can be exploited by fraudsters who, for instance, may convince people to make payments for romantic purposes or for an item posted online that doesn't actually exist. Well-known P2P platforms such as PayPal and Revolut, however, are regulated by national laws. As such, they have a responsibility to help fight financial crime, both by educating the public and by detecting potentially fraudulent activity and accounts.

Figure 6: *Consumer willingness to make P2P payments*



Changing consumer expectations

As noted previously, the survey revealed that today's consumers are a bit more cautious about sharing personal information than they have been in the past. But it also revealed that if sharing data helps protect them from fraud, they are more willing to do so.

For example, 70% of those surveyed said they would share more personal data digitally (such as location data) if it helped to provide better protection, with respondents in Brazil and UAE/South Africa being most willing (84% and 82% respectively). Just 12% of all respondents said they aren't willing to share data at all, but in the Netherlands and France, this figure is higher at just shy of 20%.

Nearly 80% of all respondents said they were willing to use security features such as fingerprints, facial recognition, hand geometry, iris recognition, retinal identification and voice recognition when completing a transaction. In fact, almost six in 10 (57%) said they preferred biometric methods to fixed passwords when authenticating a payment, compared to 35% who feel more comfortable with passwords.

These biometric methods are vital in the fight against AI-driven fraud, as explored in the sidebar, "Outsmarting the fraudsters with artificial intelligence." However, organizations must be mindful not to exclude vulnerable customers who may not be as comfortable using these types of technologies.

Regardless of the methods employed to protect customers, it's best not to create excessive friction in the customer experience. More than a third (35%) of consumers surveyed believe that longer security checks with service providers can lead to a poor experience. As a result, in competitive sectors like retail and banking, firms need to strike the right balance between enabling fast, frictionless transactions and putting in sufficient safeguards for consumers.

But fraud protections matter a great deal to the majority of those surveyed. Just 30% said longer security checks had no impact on their experience, and 27% said it provided reassurances. Given the choice, as many as 70% of respondents said they would prefer more checks, and even delays, if it meant that they received better fraud protection.

Given these findings, the best scenario is to minimize friction while maximizing security. If one provider of a product or service can offer the same level of protection (or higher), but in a more seamless way, they have a greater chance of winning out over their competitors.

Outsmarting the fraudsters with artificial intelligence

The rapid rise of generative AI tools, which can be used to rapidly create images, audio, video and content, has made it easier for criminals to commit fraud on an unprecedented scale and outwit traditional detection methods.

Identity theft, phishing communications, social engineering and document forgery are nothing new. But now, fraudsters can use generative AI to create deep fakes and large language models (LLMs) to generate highly convincing fake identities, communications, forged documents and other content at scale.

It's critical, therefore, that organizations harness the power of these same generative AI tools to stop fraudsters in their tracks at the earliest opportunity. With many scammers operating across borders, often in corrupt jurisdictions, early intervention is critical. New fraud detection technologies – which also use AI and machine learning – allow organizations to identify anomalies and trends in real time from multiple data sources and stay ahead of rapidly evolving threats.

The generative AI risk

“Generative AI and LLMs, despite their transformative potential, harbor significant fraud and security risks.

A proactive, multi-faceted approach encompassing technology, regulation and education can help mitigate these risks, ensuring trustworthy AI development and usage. By maintaining vigilance and fostering collaboration and innovation, we can harness the advantages of generative AI while safeguarding our digital ecosystems from the ever-adapting threats posed by malicious actors.

As we embrace these cutting-edge technologies, it is essential to strike a balance that allows us to progress and innovate without compromising security and integrity.”

Iain Brown, PhD, *Head of Data Science,* **SAS Northern Europe**

Finding the optimal balance

Minimize friction while maximizing security

According to Consumers International, which represents consumer groups around the world, “Consumers are often not present in financial sector regulatory decision-making in low- and middle-income countries. Nor are their experiences and perceptions directly reflected in reported metrics on consumer protection.”

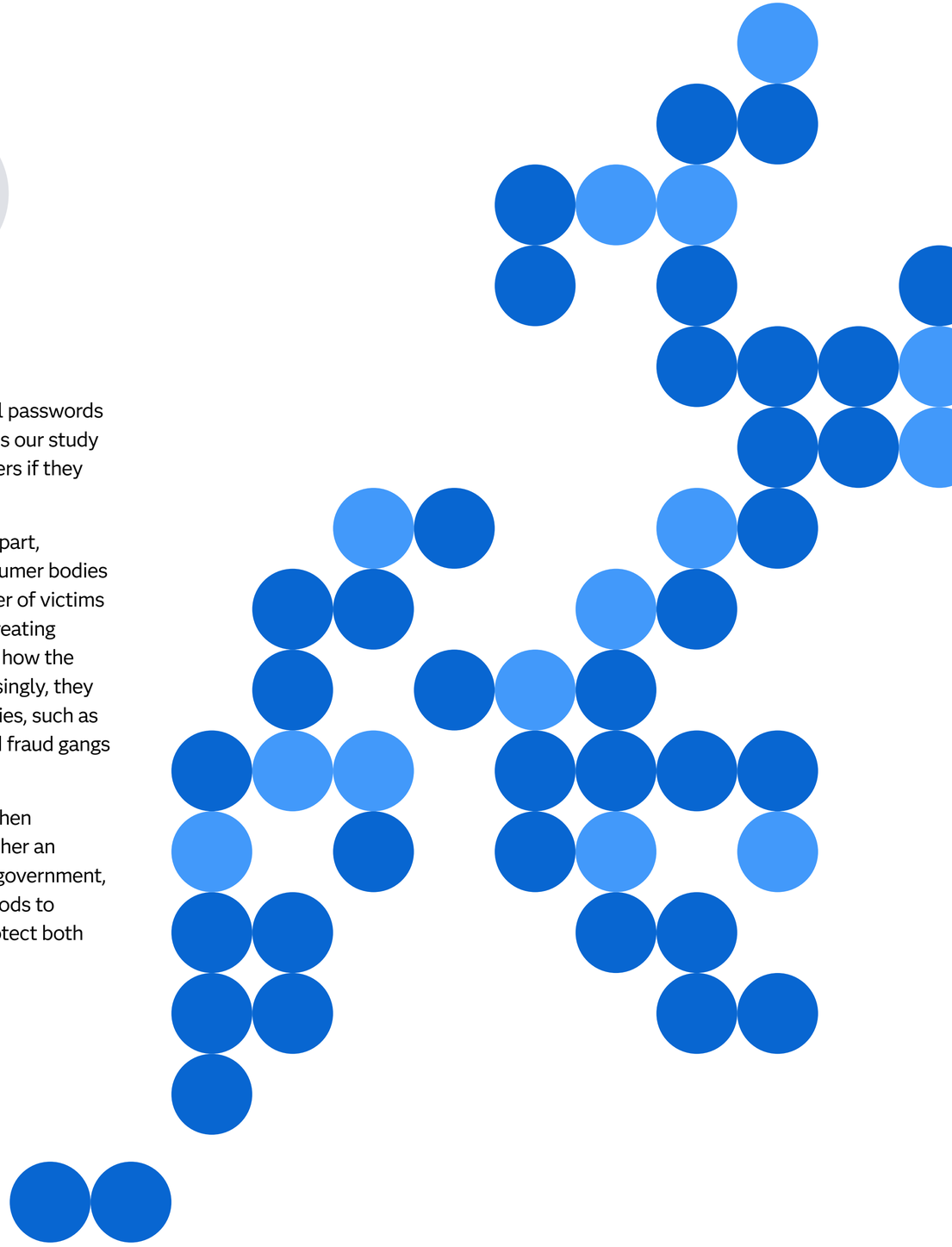
But they should be, based on the survey’s findings.

We found that the attitudes, risks and behaviors of consumers can differ greatly across different countries and regions. This is due to diverse influences such as the regulatory landscape, the adoption of – and access to – online banking tools, the effectiveness of communications around fraud risk and the social media that consumers use.

At the same time, we found that globally, consumers share many of the same concerns about fraud and risk. These commonalities indicate where businesses should focus their efforts to address consumers’ concerns about fraud. For example, they are demanding better protections – but in ways that do not make transactions with companies unnecessarily arduous. This means, for example, they would rather use biometric checks than traditional passwords because they are both easier to use and more secure. As our study suggests, consumers today are willing to switch providers if they believe another provider can offer better protection.

These changing consumer demands have happened, in part, because fraud education campaigns by banks and consumer bodies are succeeding in raising awareness – even if the number of victims and financial losses remain high. Such campaigns are creating more educated and vigilant consumers who care about how the companies they do business with prevent fraud. Increasingly, they will prefer companies that employ the latest technologies, such as generative AI, to stay ahead of sophisticated, organized fraud gangs that are exploiting the latest technology themselves.

If consumers are playing their part by being proactive, then the institutions they deal with must do the same. Whether an organization is in banking, insurance, telecom, retail or government, management must strengthen its fraud detection methods to proactively root out fraud, avoid false positives and protect both their customers’ finances and their own reputation.



Appendix A: About the study

SAS commissioned 3Gem Research and Insights to undertake a global study into some of the key trends in fraud against consumers at the end of 2022. The findings are based on a sample size of 13,500, with a 50/50 split of men and women.

Explore the survey data online at
sas.com/frauddashboard

Figure A:
Breakdown on respondents by country

UK	7.4%	1000
Germany	7.4%	1000
Sweden	7.4%	1000
Netherlands	3.7%	500
Belgium	3.7%	500
Poland	7.4%	1000
Romania	7.4%	1000
Italy	7.4%	1000
France	7.4%	1000
Spain	7.4%	1000
Portugal	3.7%	500
South Africa	3.7%	500
UAE	3.7%	500
USA	7.4%	1000
Canada	7.4%	1000
Brazil	7.4%	1000

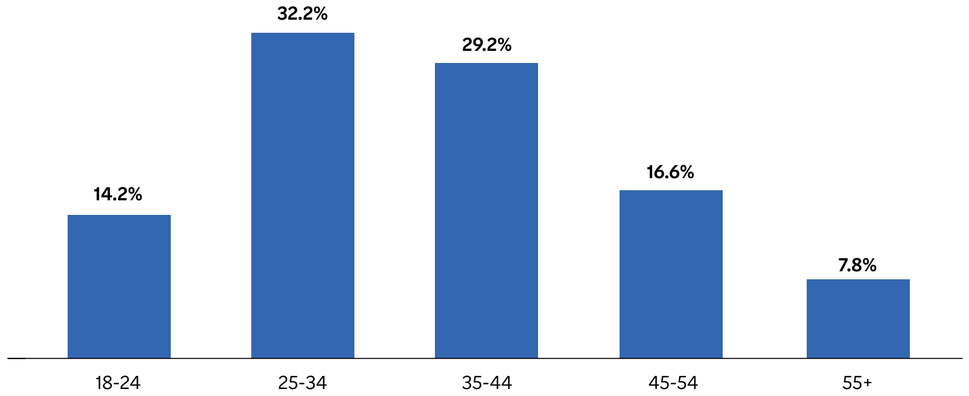
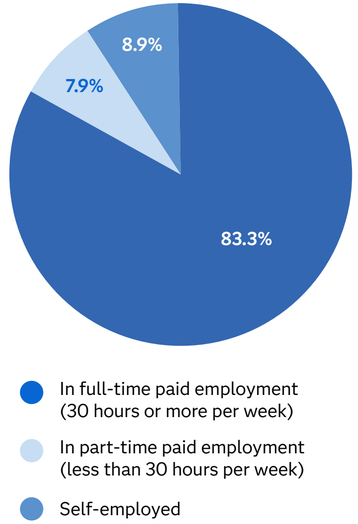


Figure B: Age breakdown of participants

Figure C:
Employment status of participants



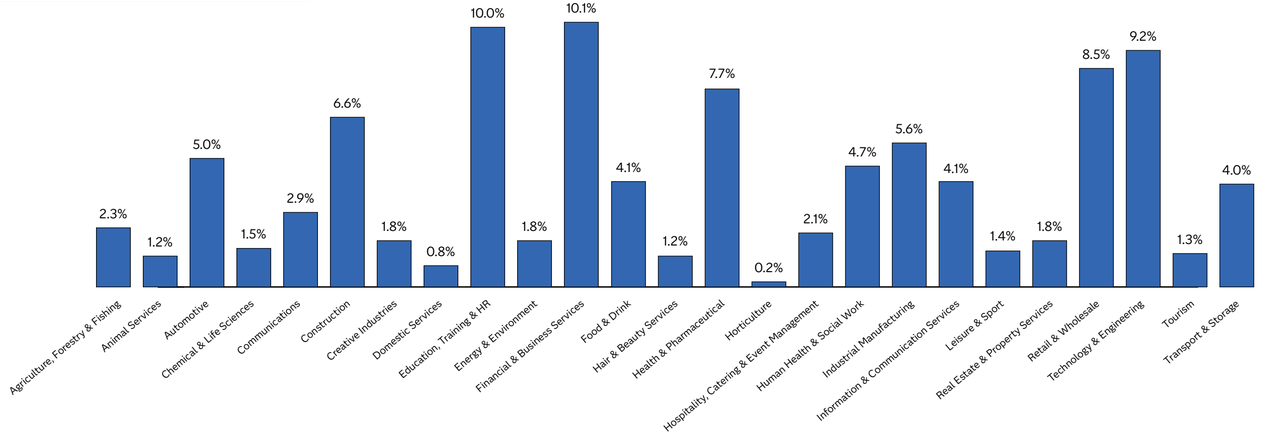
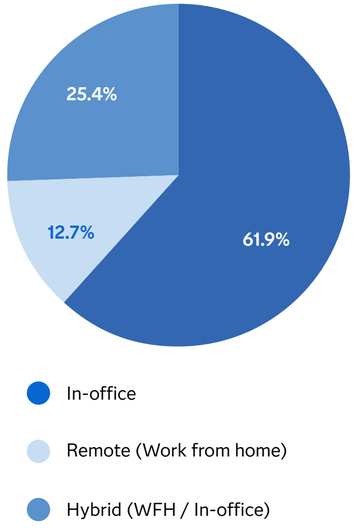


Figure D: Industry that respondents work in

Figure E:
Remote, hybrid or on-site work data on respondents



Learn more

SAS offers powerful, frictionless, AI-driven fraud detection solutions for every business. Find out how SAS' industry-leading data analytics, AI and machine learning platform can help your organization identify and respond to suspicious activity in real time, while also improving customer experiences.

To contact your local SAS office, please visit: **sas.com/offices**