The State of Digital Identity 2022

Onboarding & fraud protection – the challenges of ‘The Great Switch’

GBG

Contents

Foreword

Digital identities have never been so complex. Identities are constantly evolving - they increasingly encompass elements of our digital life, such as our digital and behavioural identities.

In 2022 and beyond, understanding digital identities will become vital for business and brand growth as digital acceleration continues at pace. The modern consumer demands a smooth onboarding experience and expects to be able to transact online securely.

If expectations are not met consumers are more than willing to ditch a brand, the State of Digital Identity Report 2022 reveals.

The brand challenge is amplified as identity fraud continues to rise. Nearly one in 10 consumers have been victims in the past 12 months. Yet almost a third of businesses still don't use an identity verification service. Businesses are finding it challenging to balance fraud prevention with managing friction for their customers.

But by understanding more about digital identities, layering the right data and having the best technology in place, companies can keep consumers safe in a digital world and keep up with evolving consumer expectations.

Over the past decade, CEOs have realised the importance of cyber security. It's now time to make identity fraud prevention a board-level issue.

Gus Tomlinson
Chief Product Officer, EMEA, GBG

Security and satisfaction:

Gaining from The Great Switch

The business landscape has changed irrevocably over the past two years. That isn't news. Our inaugural State of Identity Report in 2020 revealed that COVID-19 had been a Black Swan event for many industries, with products and services accelerated online.

This acceleration has continued at pace since 2020. What is new and will alter the way businesses operate for years to the come, is the change in consumer expectations across EMEA and all demographics.

With people accessing goods and services in the digital world more than ever before, consumers have put convenience at the core of their buying behaviours. European consumers will no longer stand for poor, confusing or time-consuming digital services.

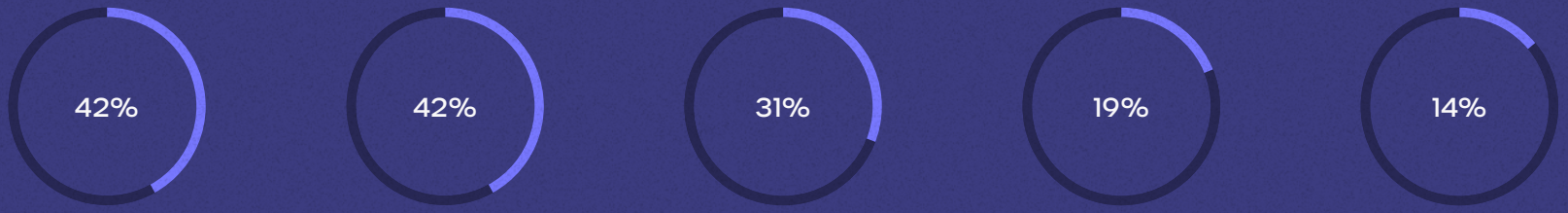
They are now more than happy to ditch a brand for a new provider. Our research reveals that during the past 12 months, it appears many consumers have decided it's time for a change.

With people spending much of their life online, they've begun to re-evaluate if they're getting the best service possible - or whether it's time to try a new provider.

Against this backdrop it's not surprising to learn that consumers we surveyed - over 2,300 of them, aged 18 and over, based in the UK, France, Germany and Spain - have been actively signing up to online accounts.

Around two thirds (66%) of European consumers did so at least once in the past 12 months. This rose to 81% in Spain, while in France the figure was lowest (45%).

Top five types of new online accounts people signed up for in the past 12 months:



It's no great leap to infer many consumers opening new accounts are moving to rival services. And with more people opening new social media accounts, the threat of people sharing their bad experiences online has increased even further for brands.

In fact, of those consumers who created a new online credit card account in the past year, 81% said they were accessing a new service - compared to just 19% who were signing up with an existing credit card. Similarly, four-fifths (80%) of consumers have signed up for a brand-new loan account online.

81% said they were accessing a new service - compared to just 19% who were signing up with an existing credit card

The results indicate we have now entered the age of **'The Great Switch'.**

If businesses offer a quick, easy and safe experience they tick a big box for consumers. According to the global trade body National Retail Federation, more than a third of individuals feel they have less spare time today compared to five years ago.

This change in their behaviour is already altering the way businesses operate, with many decision-makers realising that people will not forgive a brand for a poor customer experience.

In fact, many brands are now competing with their rivals to ensure switching is as simple as possible. Challenger banks, for example, are making it possible to ditch a high street bank and join them in just a few clicks.

Make onboarding your number one priority

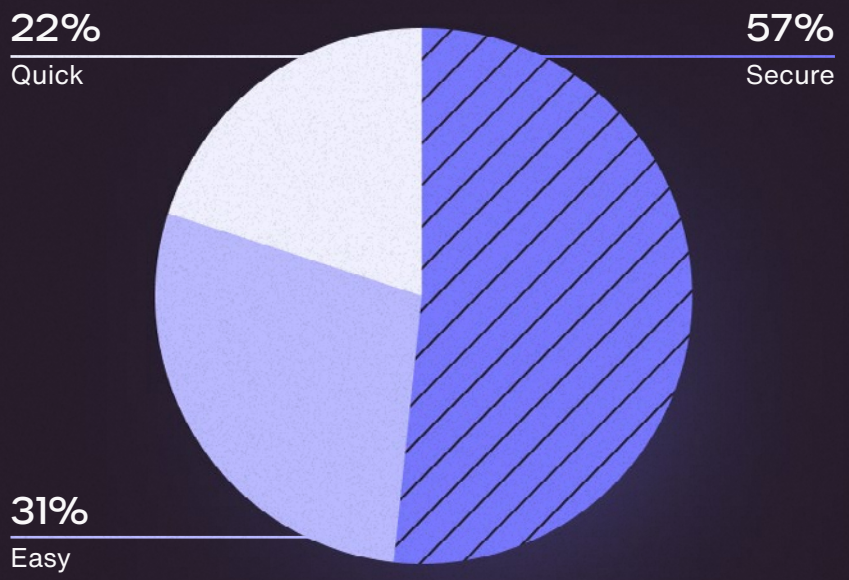
As the battle for new customers heats up, having an onboarding process that lets them sail through and sign up is crucial.

But sceptical consumers revealed there's some way to go. More than a quarter (28%) said they'd abandoned signing up for a new online account in the past 12 months because it took too long, while around one in eight (12%) stated they didn't complete registration because it was too difficult.

A major reason many firms do not deliver a satisfying onboarding operation is that they're failing to balance the twin troubles of delivering a frictionless experience while simultaneously continuing to prevent fraud.

Consumers feel strongly about these factors when opening a new online account.

How important are the following factors when opening a new account online? The process is:



Businesses recognise they have more to do in providing both a frictionless experience and protection against fraud. When asked to rate their own success at striking the right balance, on a scale from zero to 10 - with the top mark considered a friction-free approach - firms gave themselves an average mark of just six.

If businesses want to protect their brand and continue to grow, they must do more to improve that onboarding experience.

Getting this wrong can cost businesses thousands, if not millions. According to digital marketing agency WebFX, the average small and medium-sized business (SMB) spends between $9,000 and $10,000 on Pay Per Click (PPC) every month trying to drive customers to their websites. Larger businesses will spend more. However, in our experience, 80% of those leads are lost if a business asks a consumer to complete a manual onboarding process.

> The average small and medium-sized business spends between $9,000 and $10,000 on Pay Per Click every month

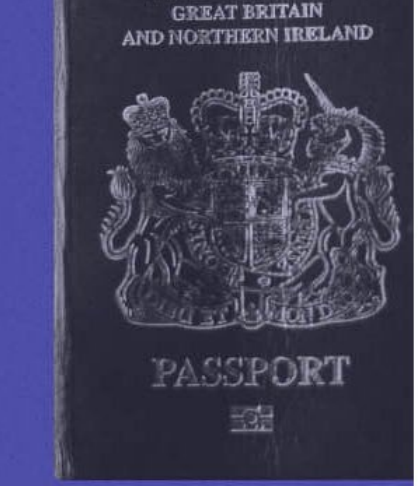
The modern consumer is more than happy to walk away from a poor experience or process. And, with the onboarding experience often the first interaction a customer has with a brand, this will not only lead to lost custom in the short term but could also damage a brand in the long term.

As a result, the ability of businesses to successfully tap into The Great Switch could mean the difference between fortune and failure in this new golden era of eCommerce.

Switchers' behaviour can therefore be a precious commodity for companies - but they must do everything they can to ensure it's not sacrificed through substandard service which swells the dropout rates that are such a problem for many brands.

Digital identity's next step:

Mobile and alternative data



By 2026, it's expected there will be more than 826 million smartphone users in Europe. It's no surprise, therefore, that much of The Great Switch is taking place on mobile devices.

More than three quarters (76%) of consumers surveyed who have signed up for a new online account in the past 12 months said they did so via an app or browser on their device. The figure reached 82% in Spain.

The survey revealed some interesting insights into how consumers use their smartphones.

People generally like to stick with the same mobile if they can: those surveyed have kept theirs for an average of six years. Just 12% have bought a new one in the past 12 months.

It's also fascinating to note how users feel about the ease of completing a range of tasks on their smartphone. Mobile banking (47%) was the activity most frequently rated 'extremely easy' by those surveyed, with shopping/making purchases (46%) close behind.

> 76% of consumers who have signed up for a new online account in the past 12 months did so via an app or browser on their device

The two tasks least likely to be deemed extremely easy were crypto/forex online trading (13%) and online gambling (20%).

> Around two thirds (67%) said they conduct business in the mobile environment

Generally, consumers found all the listed activities manageable, with online trading recording the highest proportion of consumers (8%) who claimed it's 'not at all easy'.

Companies recognise mCommerce is now a major route to market: around two thirds (67%) of those surveyed - out of 160 decision-makers at firms in various industries across Europe - said they conduct business in the mobile environment. France (79%) is the most advanced market in this regard. The UK (65%) is a little way behind while Germany (56%) is playing catch-up.

With the mobile now playing such a key role in day-to-day digital life – with people banking and shopping, arranging doctor's appointments, ordering takeaways and more via their smartphone – businesses must now consider how they can leverage this to both improve onboarding and also better protect customers from fraud. And, ultimately, provide a great customer experience.

Mobile phones have become a natural extension of our identities, and now more than ever they provide a key part of the puzzle when building trust in a digital world and enabling consumers to transact online with confidence.

After all, your identity is about much more than your date of birth, your passport or your identity number. It varies by demographics, psychographics and industry.

The one constant is that the complex set of data points that shape our identities are vital in keeping the wheels of commerce turning. Mobile data can form a vital layer in better understanding an individual.

Businesses can prevent fraud by being confident in their ability to verify an individual – so they can let the good guys in and keep the bad actors out. Identities are often verified through physical documents (passports and driving licenses) or credit history. However, the data created by our use of mobile phones could act as an additional layer of alternative data to increase confidence in identity verification.

This can also help spur social inclusion, helping the millions of people who do not possess identity documents, such as passports or driving licenses, get access to digital goods and services.

After all, a mobile number is personal to an individual - and mobile is becoming the primary enabling platform in our lives. Knowing that a person is the owner of that number is a robust way of validating and authenticating an identity and preventing sophisticated fraud across channels such as online, call centre and in-branch. And, as technology improves the reach and adoption of mobile, the insights generated increase.

How mobile can help prevent emerging fraud threats

Synthetic Identity Fraud

23% of businesses see synthetic identity fraud as the most prevalent fraud scheme in their industry

How to tackle with mobile

The creation of synthetic, or fake, identities can cause havoc when it comes to fraud and money laundering. Criminals are increasingly attempting to plant synthetic IDs into traditional data sources, so that companies can be tricked into thinking these IDs are real. By using mobile data including Proof of Ownership, Carrier Type and SIM Swap as an extra layer of verification, businesses are able to identify suspicious-looking identities at the point of onboarding.

Social Engineering

27% of businesses see social engineering as the most prevalent fraud scheme in their industry

How to tackle with mobile

Fraudsters can attempt to access accounts, or purchase items, and acquire crypto wallets using confidential information they've gained by manipulating people. A range of methods can help to tackle this. By using mobile technologies such as silent mobile authentication, SIM swap and call forward signals companies can more confidently transact with their customers.

Authorised Push Payment

14% of businesses believe push fraud poses the biggest risk to their industry over the next three years

How to tackle with mobile

According to Which?, "An authorised push payment (APP) scam, also known as a bank transfer scam, occurs when you - knowingly or unwittingly - transfer money from your own bank account to one belonging to a scammer."

This kind of fraud is particularly malicious and has been on the rise since the start of the pandemic, with fraudsters preying on people's vulnerabilities and taking advantage in the rise of eCommerce. Most brands are taking steps to stop this already, but an emerging set of data called "Line Busy" could help combat this fraud. This approach connects businesses with operator networks at the time of transaction to understand if an individual is currently on a phone call - a powerful signal used in fraud detection.

Identity fraud:

It’s a matter of when, not if

As people have become more reliant on the internet for everyday tasks since the pandemic began the prevalence of identity fraud has spiked. In a recent report, the UK's Office for National Statistics found a 14% increase in total crime in the year to September 2021, driven by a 47% increase in fraud and computer misuse, which surged during lockdown.

With more activity than ever being conducted online, there are huge vectors of vulnerability for criminals to target as they seek to exploit holes in firms' digital footprints.

The consumers we surveyed confirmed fraud is a constant concern for them. Almost one in 10 (9%) became a victim of it in the past year and a further 18% couldn't be sure if they had been scammed or not. UK and German consumers (both 9%) were the most likely to be victims of fraud. In Spain, the figure was 8% and in France, it was 7%.

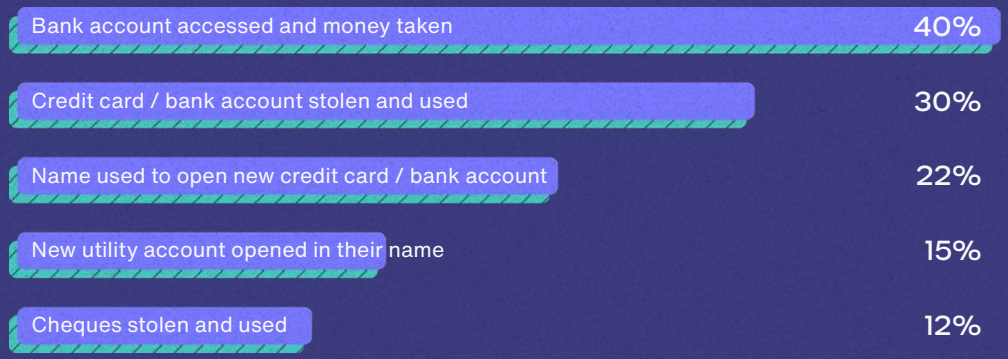
> Almost one in 10 (9%) became a victim of fraud in the past year

Assessing the impact of fraud

Consumers have suffered in several distressing ways from the consequences of identity fraud during the past year. The survey results underscore the fact that fraud is not a victimless crime.

Consumers also worry about future fraudulent activity. A total of 92% were concerned they'll eventually be hit by it, including nearly a fifth (19%) who said they were extremely concerned.

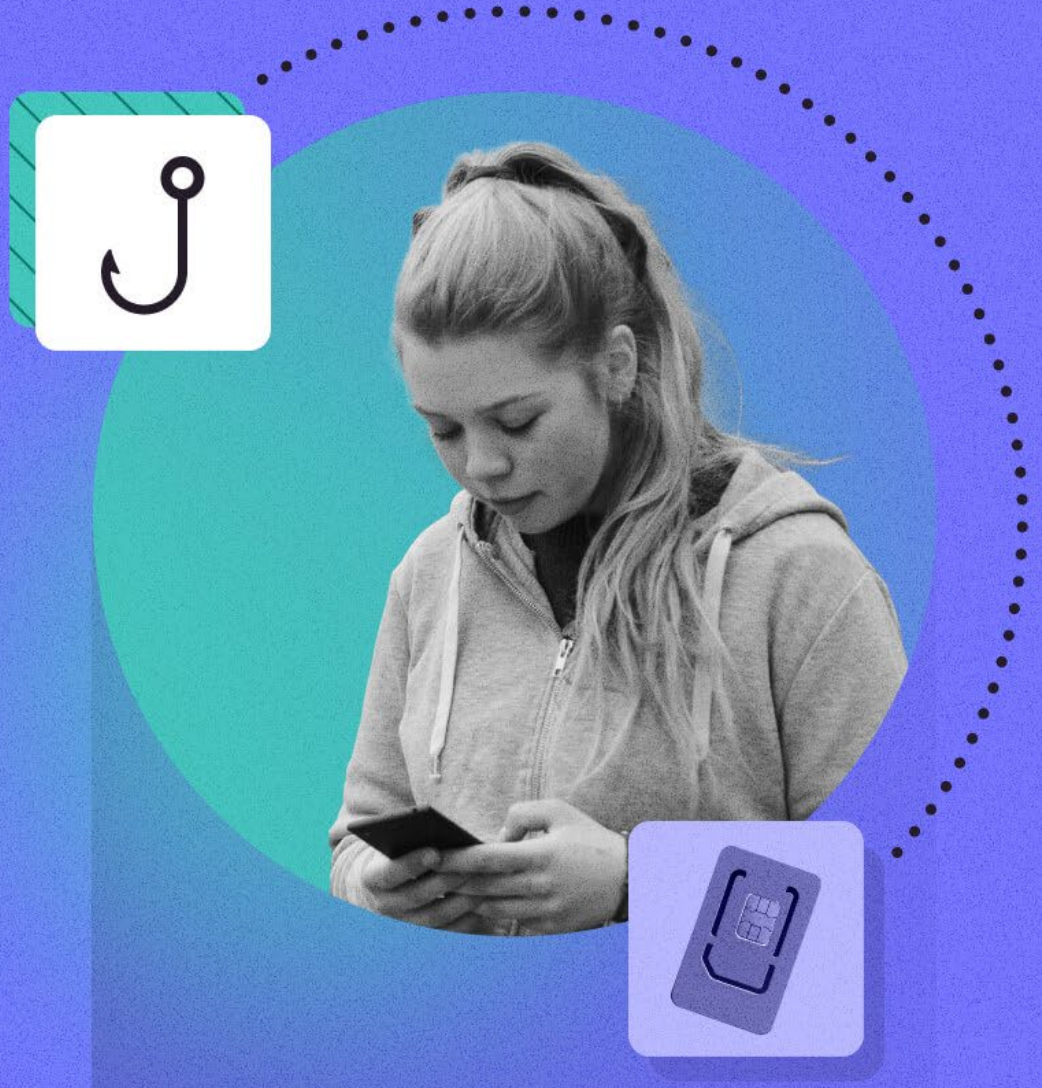
Consequences for fraud victims in the past 12 months:



Worryingly, becoming a victim of one type of fraud can lead to a consumer being left vulnerable to further criminal activity. For example, having your mobile stolen or cloned could enable a fraudster to access a bank account, or even give them access to enough personal details to be able to open a completely new bank account or take out a loan in the victim's name.

Young adults:

The biggest victims of identity fraud?



There's evidence in our research to suggest younger consumers are the most likely to be a victim of identity fraud.

Overall, nearly one in eight (13%) people aged 18 to 24 across Europe have been victims of fraud in the past 12 months, but this rose to almost a fifth (18%) in the UK and 24% of young consumers in Spain.

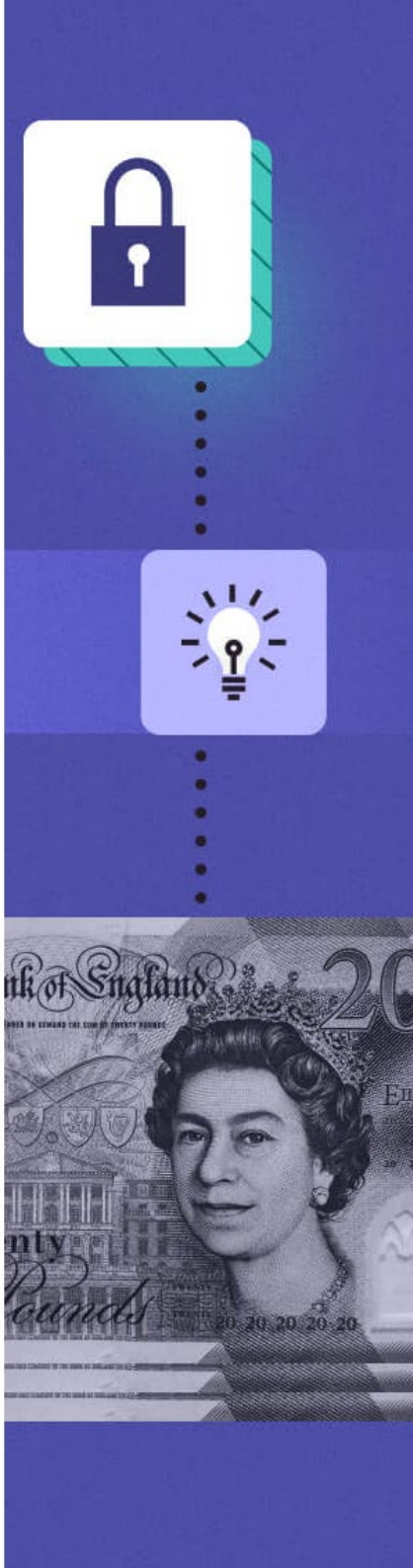
The likelihood of being a fraud victim seemingly decreases with age. Among 25- to 34-year-olds, 12% said this has happened to them in the past year. The figure for those aged 35 to 44 was 9%, dropping to 7% of 45- to 54-year-olds, and just 4% of consumers aged 55 and over.

> Nearly one in eight (13%) people aged 18 to 24 across Europe have been victims of fraud in the past 12 months

Almost half (48%) of consumers aged 18 to 24 who suffered a breach of their bank account in the past year had money transferred out by fraudsters. Meanwhile, more than one in seven (15%) stated a new utility account was opened in their name.

Young adults are often labelled by businesses as the most tech-savvy demographic. But there is a large section of this age group who believe dealing with online security should be companies' responsibility, rather than them looking after it themselves. Only 62% of young adults believe it's their responsibility to protect their own information, compared with an average of 76% across all age groups.

Despite this, 94% of the youngest age group surveyed were concerned about potential online fraud affecting them in future - so the issue is clearly front of mind.



The threat for young adults looks set to continue, unless businesses up their game and also educate people on the need to protect their own information too. With young people spending so much of their time online, there are naturally more potential touchpoints for fraudsters to target. Meanwhile, older generations tend to be naturally less trusting of digital, so some fraudsters may see young adults as an easier target.

Thankfully, some businesses are realising fraudsters are targeting younger consumers and are taking active steps to stop them. For example, UK dating app Fluttr ensures anyone signing up must complete biometric identity verification before they're allowed to contact other members.

> Only 62% of young adults believe it's their responsibility to protect their own information

What is clear is that younger adults have less transaction history and therefore less established digital identities. This only compounds the fraud threat, as it makes it easier for criminals to manipulate systems and potentially impersonate a real person or take over an account.

Businesses need to do more to understand the data points that make up the identity of young adults. But this is another area where layering data about a person's mobile usage can help. It can help businesses understand more about the individual, making it easier to securely verify them and provide a better customer experience. And, with more 18- to 24-year-olds having a mobile phone than a driving licence, it could provide a powerful tool for businesses in the fight against fraud.

Satisfying younger consumers can also help brands tap into potential lifetime customer value; this is reflected in the models of digital-only banks and other challenger brands which know these consumers hold the spending power of the future in their hands.

Time to take fraud seriously

Our findings should be a stark warning to businesses that they must take steps now to build trust in their digital services. This means demonstrating they can accurately identify an individual thereby stopping fraudsters in their tracks. Customers will also want to know their information is being kept safe.

Frankly, any organisation that does not think it will encounter fraud attempts in the near future is deceiving itself. More than a quarter of businesses (27%) said that fraud has increased in the last year.

Fraud is rife: almost half (42%) of all the firms surveyed reported that they had experienced known or suspected attempted fraudulent activity in the past 12 months. In France, 64% of companies claimed they had experienced this type of criminal activity.

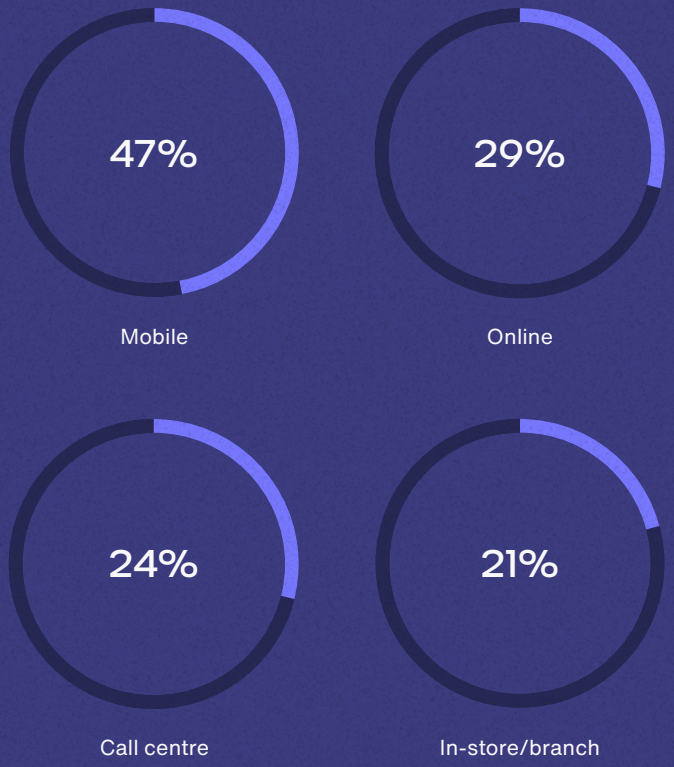
In reality, these figures are likely to be much higher – some companies aren't prepared to reveal they've been hit by criminals or are simply unaware of the fraudulent activity that has taken place.

Preventing fraud saves money but also builds the confidence of customers. Anything businesses can do to verify an honest customer and give them a better journey builds revenue, trust and value.

For example, a customer's lifetime value might be four times the cost of identity fraud using their details. If fraud can be prevented, their overall value to the business jumps by a quarter.

Our online Identity Fraud Calculator helps businesses to understand how much fraud is costing their organisation.

Percentage of businesses that say fraud has increased across these channels



Counting the cost of identity fraud

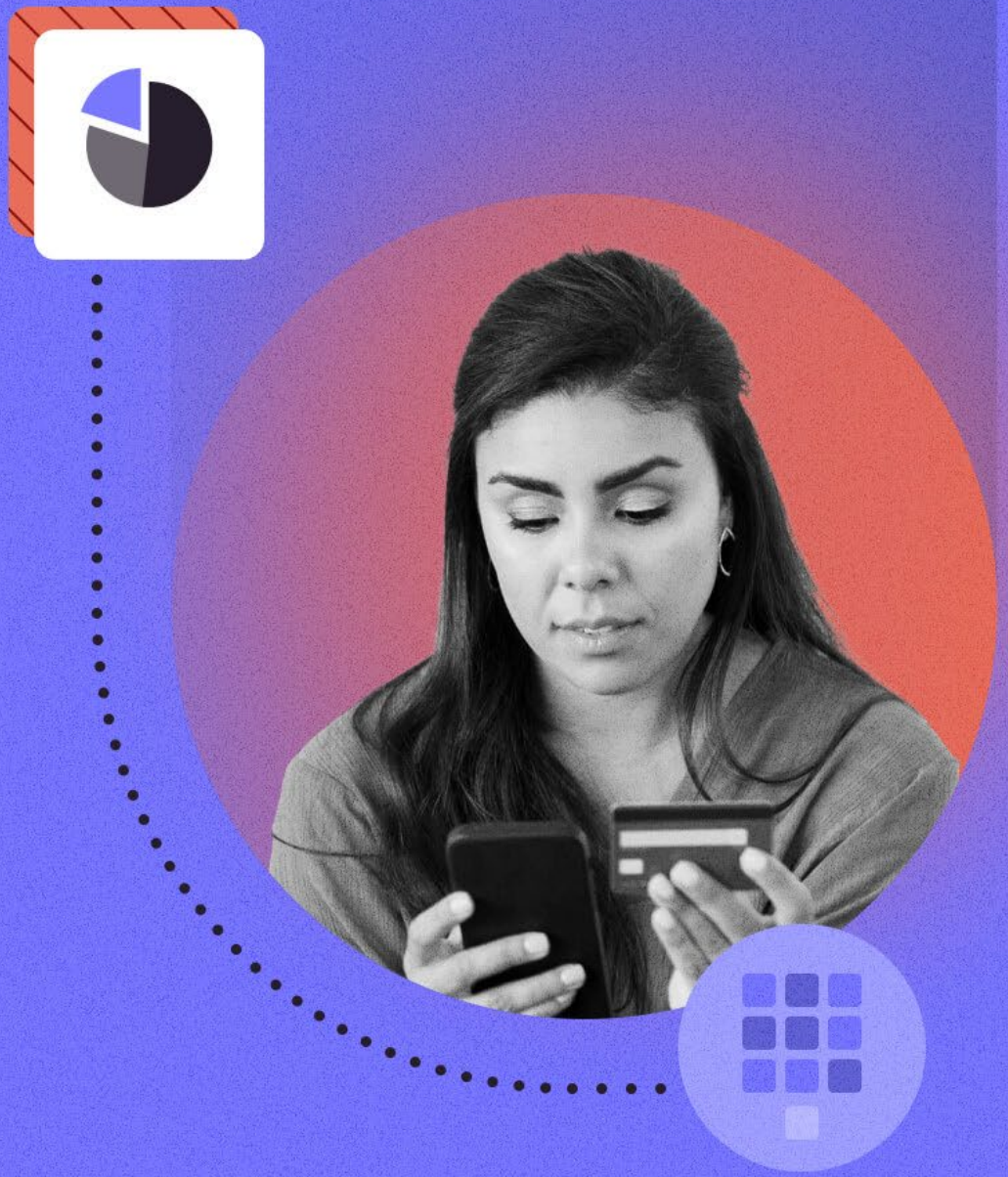
The fallout from fraud shouldn't be taken lightly. Firms experiencing a known or suspected fraud attempt said the average transactional value of a breach was just short of £16,000. This rose to more than £23,000 in France.

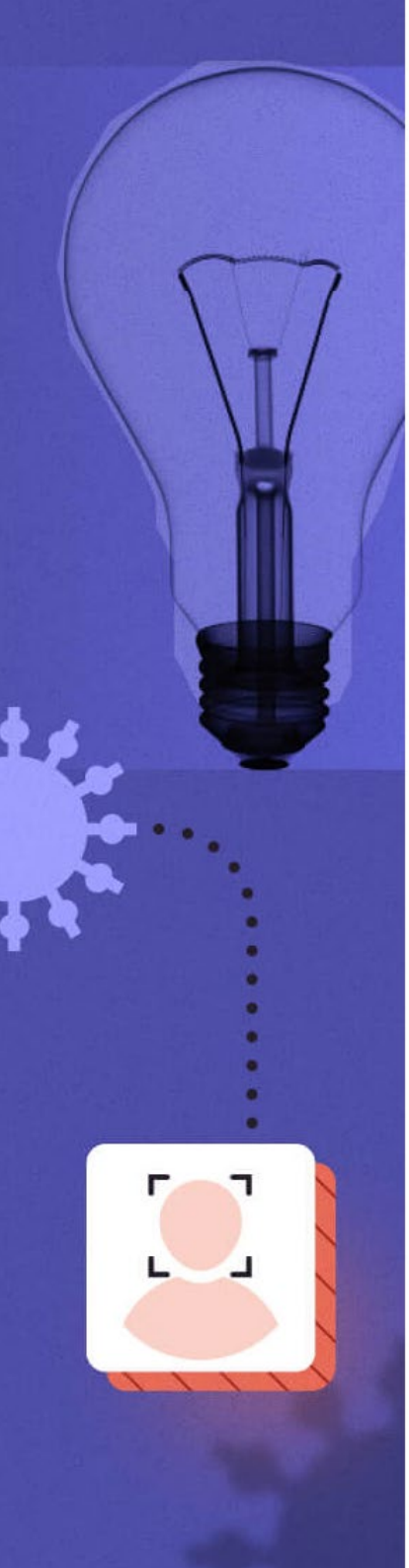
Meanwhile, 15% of these companies lost between £35,000 and £50,000 on average, revealing the sophisticated nature of breaches. A further quarter (25%) claimed each breach cost their business between £10,000 and £34,999.

Firms are aware they are fighting fraud on many fronts - in fact, every customer touchpoint is under threat. By embracing digital identity and improving identity verification, however, businesses will be better placed to prevent the growing threat of increasingly sophisticated fraud attempts such as social engineering, SIM swap and synthetic fraud.

All in all, fraud isn't just big business for criminals - it's a huge problem for business.

Fraud and financial services





Advances in digital technology and consumer interest in online services have disrupted the financial sector during the past decade.

The pandemic has solidified this shift to online banking and trading. According to a MasterCard study, 87% of European consumers who switched their financial activity to digital channels as a result of COVID-19 expect to continue using banking apps as life gets back to normal.

But with this big change in behaviour comes greater customer expectation. In a YouGov survey, 81% of UK adults said the quality of an online experience determines who they bank with.

Businesses that fail to heed these warnings will struggle, including financial services brands as consumers demonstrate their desire for a variety of digital banking and trading options.

Many digital financial services providers are currently finding favour among consumers -people seem largely happy with the ease and security of accessing online accounts.

> 81% of UK adults said the quality of an online experience determines who they bank with

With 74% of mobile users deeming mobile banking very or extremely easy, it was seen as being almost as simple as mobile shopping (77%). Peer-to-peer payment (P2P) services such as PayPal (68%) also fared well on this measure.

Ease of trading - crypto or forex - (28%) and gambling online (40%) were perceived as somewhat less simple.

Mobile users were also more sceptical about the security aspects of accessing certain financial services via their device. An equal share of consumers (54% each) named mobile banking and also P2P payments as very or extremely secure. Mobile shopping scored 53% on the same measure.

A notable 29% of consumers said they would be more likely to use a financial institution if they were aware the company was using advanced identity verification methods for account registrations. This figure rose to 35% of consumers in France, and 31% of both men and those aged from 45 to 54.

Because simplicity and security combine to build consumers' trust in a business it's vital companies take steps to deliver both successfully at the top of the funnel, which would boost the satisfaction ratings shown in the survey results.

On both factors, there is plenty of room for improvement. While nearly two thirds (64%) of mobile users who signed up for new financial accounts rated their experience very or extremely easy just 44% of consumers believed registering for new accounts via their mobile was so simple.

Financial sector businesses have a duty to keep customers' information safe and establish their true identities to clamp down on growing levels of fraud. At present, businesses score themselves just five out of 10 when it comes to taking a strategic, comprehensive approach to these vital aspects of online operations. This is despite 66% recognising that identity verification can be a competitive advantage.

Technology has a huge role to play in digital identity compliance and verification. Cutting-edge solutions keep customers engaged while increasing conversion rates by:

Delivering great customer experiences
Dynamic, frictionless, user-friendly onboarding

Keeping companies fully compliant
Anti-fraud security without compromising on convenience

Building customer trust in brands
State-of-the-art document verification and data management

Forex and crypto playing catch-up

The survey results show that emerging online trading services have some way to go to ensure they can provide a customer experience that is both smooth and secure.

Fewer than half (42%) of consumers said it's easy to use crypto or forex services on their phone, meaning they rank it - at best - half as easy as every other financial services activity they were asked about. The only exception was online gambling, which 55% said was easy.

Consumers in Spain were the least likely (27%) to rate crypto and forex services as being easy to use on their mobile. This compared to 42% in Germany, 46% in France and 59% in the UK.

With more than one in 10 (11%) consumers signing up for a new crypto or forex account online during the past year it's clearly a growing part of the sector. There's work to do to improve the onboarding process, making it slick and secure in order to persuade people to trust the brand they're signing up to - especially when potentially large sums of money are being moved around.

Mobile can play a key role in changing perceptions and building trust in crypto and forex - just as it can in other digital-first sectors such as eCommerce.

2022 identity fraud threat matrix

As the threat matrix below highlights, companies must not only combat key threats today - they also need to keep up with the identity challenges of tomorrow. Balancing friction, fraud prevention, compliance and a delivering a great CX are leading commercial considerations of the digital era.

Today's most prevalent fraud threats

Established approaches

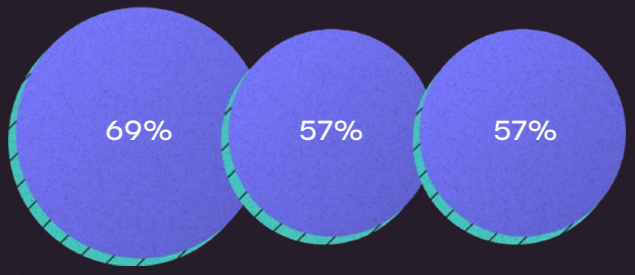
Businesses 'most likely to use'

Device authentication

Third-party databases

The digital identity core

Most important to my identity today



Date of birth

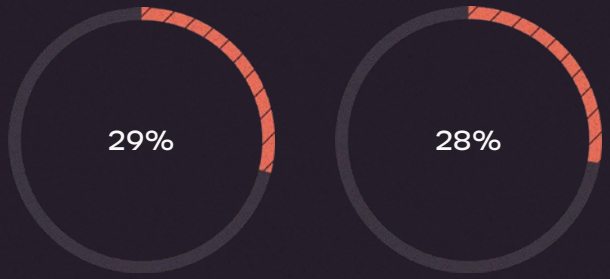
Identity number
e.g. National Insurance

Passport

Tomorrow's identity trends

Emerging approaches

Businesses 'least likely to use'

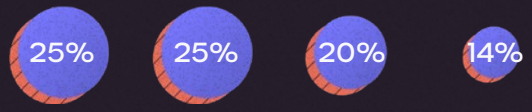


Name

Detecting genuine presence

The digital identity fringes

Becoming important to my identity

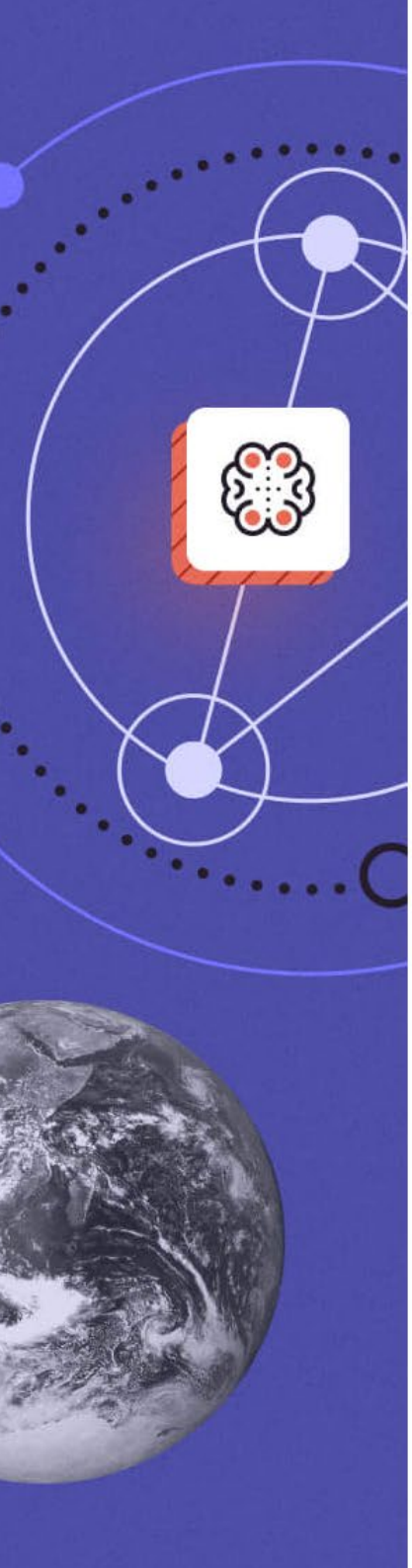


Family information
e.g. name

Assets/ financial accounts

Employer

Social media profile



The future of digital identity

Digital identity has a major part to play in future economies. Governments and businesses across the world realise this.

In the UK, for example, the government published the second version of its digital identity trust framework last year. This framework is part of plans to "make it faster and easier for people to verify themselves using modern technology through a process as trusted as using drivers licenses or passports."

However, if we are to make the world easier to navigate for both private businesses and the public, while keeping them safe from fraud, we must make data, in particular government-held data, more accessible.

The UK Government, for example, has a complete and accurate set of data that could be used to bolster somebody's digital identity. Currently, access to this data is limited and businesses, and the government, are therefore limited in what they can deliver when it comes to digital solutions. Often, identity is still verified through physical documents or credit history checks – but this can leave 'thin file' people, or those without a driving licence or passport, excluded from digital society.

If trusted private companies could securely access databases that cover all demographics of the UK population, we could bolster the economy while making the digital world more secure. Moving house, changing jobs, picking up medication, or applying for a tax rebate, are all things that could be made simpler and easier when access to data is increased and digital identities are used. It would also make it easier for organisations to innovate digitally, making it a simpler safer world for consumers and businesses.

Time to build trust in a digital world

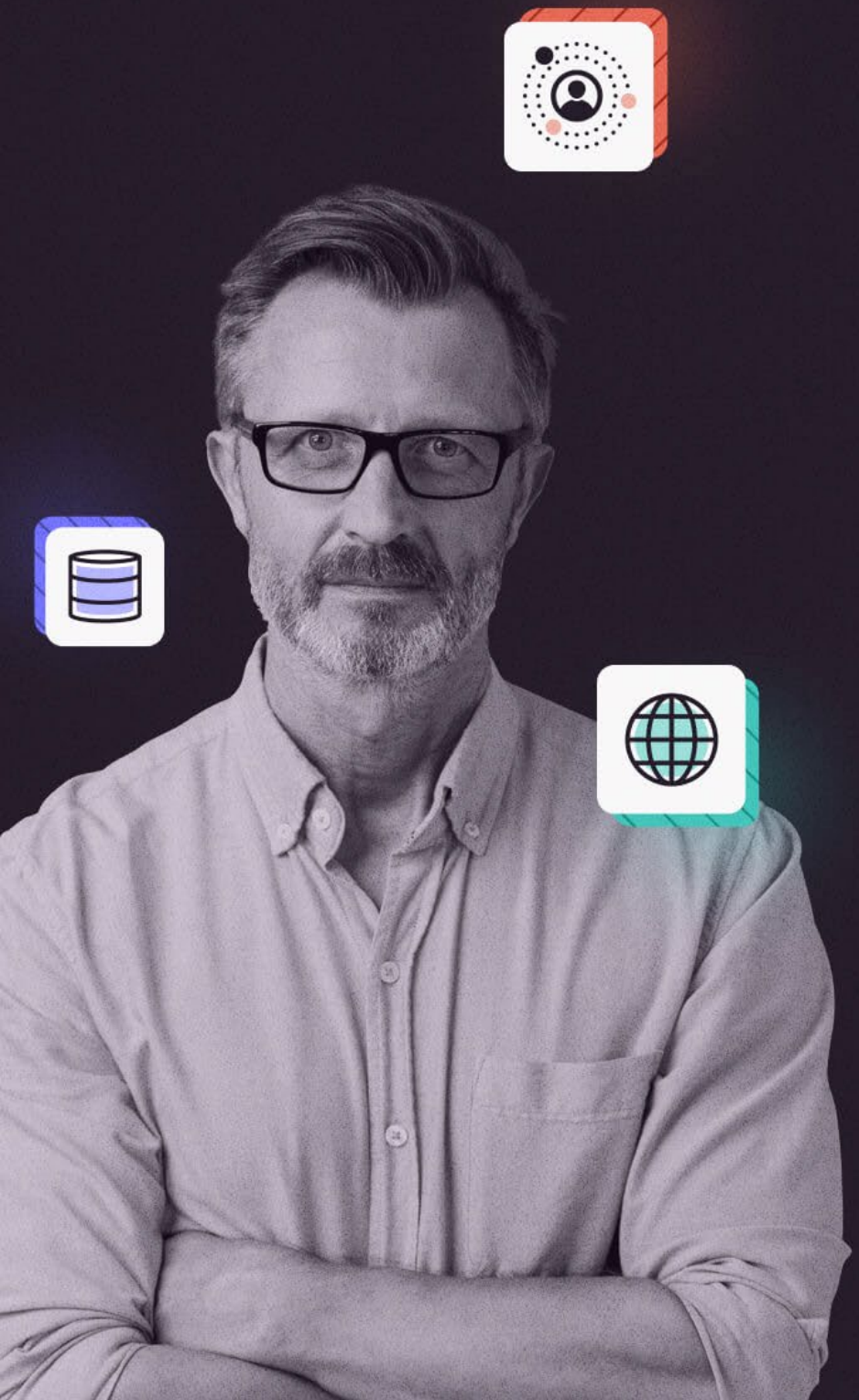
If businesses want customers to continue to use their digital services they must start to build more trust so that people can transact online with confidence.

To do this, they need to get better at identifying, onboarding and - most importantly - protecting their customers.

Many of the 64% of firms using third-party or in-house identity verification services are already realising the benefits. Ensuring every new customer is who they say they are while balancing checks with a satisfying onboarding experience is key to building trust and revenues.

However, many businesses are facing challenges when it comes to digital identity. Nearly six in 10 (59%) companies claimed data coverage - the availability of data from different geographical reasons, in order to serve a global customer base - was an issue for them, and almost as many (58%) cited the quality of data as a challenge. Meanwhile, match rates were deemed a problem by 42%.

Benefits of using an identity verification service



All of these perceived difficulties link directly to the efficacy of onboarding processes. But there are strategies to pursue that will help solve the puzzle of identity verification:

1 **Seek alternative data sources**

Traditional methods of identity verification are no longer enough to confidently verify all individuals operating online. Businesses must layer these traditional sources with alternative identity data, such as mobile data, social media data and utilities payments.

2 **Layer data and use technology to trust decisions**

By combining traditional data with alternative data, businesses can construct a richer, contextual understanding of individual consumers, simultaneously enabling more accurate risk assessment and personalised customer experiences.

3 **Take an incremental approach to establishing customers' trust at each stage of their journey, stepping up security along the way**

By being transparent and clearly detailing what data is being collected, analysed and why, businesses can begin to build trust with consumers and take steps to prevent fraud.

It's clear that many businesses recognise the need for action when it comes to identity and fraud prevention. However, if we are to build trust in the digital world, there is still plenty of work to do.

Worryingly, just under one third (31%) of companies don't use an identity verification service. Without it, they cannot be confident that they are letting the good guys in and keeping the bad guys out.

And with customers more willing to ditch a brand than ever before, security and fraud protection could become key competitive differentiators. Failing to act now may make your business the next in line to fall victim to the consequences of the Great Switch.

Methodology

The research, consisting of two separate projects, was conducted by Censuswide, with 2,362 smartphone owners aged 18+ sampled in the UK, France, Germany and Spain between January 17 and 26 2022. 160 decision makers in insurance, financial services, eCommerce/retail, fintech, gaming/gambling and the pension sector across UK, France, Germany and Spain were also surveyed between January 17 and 26 2022. Censuswide abide by and employ members of the Market Research Society which is based on the ESOMAR principles.

GBG

gbgplc.com