DIGITAL IDENTITY

DIGITAL IDENTITY

Distributed in THE TIMES

Published in association with IDENTITY WEEK GLOBAL • TRUSTED • VISIONARY, infosecurity STRATEGY | INSIGHT | TECHNOLOGY, MONEY 20/20 BY ASCENTIAL

Contributors

Francesca Cassidy
Raconteur's deputy editor, she contributes to a range of business and consumer-facing publications.

Christine Horton
Long-term contributor to specialist IT titles, she writes about technology's impact on business.

Oliver Pickup
Award-winning journalist, specialising in technology, business and sport.

Daniel Thomas
Writer and editor, with work published in *The Telegraph*, *Newsweek*, *Fund Strategy* and *EducationInvestor*.

Jonathan Weinberg
Journalist, writer and media consultant/trainer specialising in technology, business and the future of work.

Emma Woolacott
Specialist technology writer, she has contributed to *Forbes* and the *New Statesman*.

Nick Easen
Award-winning writer and broadcaster, he has produced content for *BBC World News*, *CNN* and *Time*.

Duncan Jefferies
Journalist and copywriter writing for *The Guardian* and *Independent Voices*.

Amelia Tait
Journalist published in *Wired*, *The New York Times*, and *MIT's Technology Review*. In 2020, she was named one of Forbes' 30 Under 30 in Europe.

Sanjana Varghese
Technology, culture and politics journalist, with work featured in *WIRED*, *Vice* and *New Statesman*.

Davey Winder
Award-winning journalist and author, he specialises in information security.

Abby Young-Powell
Journalist with work published in *The Guardian*, *The Independent* and *Positive News*.

raconteur reports

Lead Publisher
Emma Ludditt

Managing editor
Sarah Vizard

Associate editor
Peter Archer

Deputy editor
Fran Cassidy

Production manager
Hannah Smallman

Design
Sara Gelfgren
Kellie Jerrard
Colm McDermott
Samuele Motta
Nita Saroglou
Jack Woolrich

Art director
Joanna Bird

Design director
Tim Whitlock

@raconteur /raconteur.net @raconteur_london

raconteur.net digital-identity-2021

UK ECONOMY

Unleashing the UK's digital identity economy

The UK government is planning an overhaul of digital identity in 2021, but it faces a number of obstacles if it is to succeed

Christine Horton

The UK faces urgent challenges if the benefits of a secure and efficient digital identity protocol are not to be squandered.

Critics are calling on the government to ensure the right technology, processes and standards are in place to unleash a new, effective and prosperous era of digital identity.

Westminster has announced plans to "unlock the UK's digital identity economy". Proposals include updates to existing laws to enable digital identity to be used as widely as possible, alongside a new set of guiding principles for policy development.

Digital infrastructure minister Matt Warman says the goal is to make it easier for people to prove their identity online to enable faster transactions. He knows digital identity "has the potential to add billions to our economy".

This follows a surge of people turning to digital services during the coronavirus pandemic. Some 2.6 million people made an online claim for the Self-Employment Income Support Scheme between its launch in May and September 2020. According to the Department for Digital, Culture, Media & Sport, 1.4 million claimants had no prior digital identity credentials and needed to pass through HM Revenue & Customs' identity verification service.

The new framework is long overdue. A report from think tank Policy Exchange says the lack of reliable digital ID services is severely limiting the UK's future as a leading digital economy.

Last year, the Cabinet Office's annual report said the government's current digital identity programme, GOV.UK Verify, "continued to pose notable risks", as it struggled to cope with demand for digital services in the early stages of lockdown.

"It's a shame that the UK lost so much time on the unsuccessful Verify project. But there's more energy and appetite now in government to tackle digital identity than we've seen for many years. Let's hope this moment won't be wasted," says Jessica Figueras, a technology strategist specialising in government, policy and regulation, and author of the local authority digital identity survey *Identifying as Citizens*.

So what can we expect from the rollout of a digital ID scheme in 2021?


Paul Burlington via Unsplash

The government has already ruled out a physical or biometric ID card scheme, as used in other countries.

"The debate about digital ID has always been politically difficult in the UK," says Figueras. There have been long-standing fears about privacy and possible government overreach. Remembering the strong historical opposition to ID cards, this has translated into a push back against centralised digital ID schemes based on a single citizen database.

"This is why governments over the past decade have consistently tried to implement a so-called federated approach to ID, which allows citizens to be identified without relying on a database that consolidates lots of data about them in one place," says Figueras.

Colin Wallis, executive director of the Kantara Initiative, a global non-profit association dedicated to improving trustworthy use of identity, agrees the UK won't be looking at just one digital ID scheme.

"If you are not operating a single scheme as is the case with the common law countries, most notably Australia, Canada, New Zealand, the UK and United States, you are not operating a single scheme. Instead, you are operating or supporting the operation of several schemes by providing the basic requirement: a secure and private attribute exchange of authoritative government-held identity-related data," he says.

"With the UK, United States and New Zealand in a similar position in their approach to legislation at a similar time – Australia and Canada are further advanced – it would be sensible for the UK and United States to align."

There will, of course, be challenges for the government. For example, there are issues of digital exclusion, where people don't have the paper credentials that digital services will be relying on to identify them, such as passports and driving licences.

"Very often these are citizens who are vulnerable in other ways: homeless, elderly or have an irregular immigration status. Things can go badly wrong for these people when they're not able to prove their identity, as we learnt from the Windrush scandal. So it's even more important that public service providers can offer them an appropriate service," says Figueras.

Elsewhere, the government is challenged with maintaining regulatory oversight of the digital ID landscape. The federated path the UK has chosen is more complex than a highly centralised system seen in countries such as Estonia, which has built a trailblazing digital society. This means the user experience in the UK may be more fragmented. There may also be dependencies between public and private sector bodies that might not always be clear.

Ultimately, the goal for the government is to offer a digital ID service that supports users across both public and private sector organisations, enabling the sharing of data with trusted third parties.

For example, industries that require formal proof of identification for regulatory purposes, such as banking, could integrate with the digital ID service to fast track such processes, assuming the user has opted to allow their data to be shared in this way.

"It also represents a great opportunity to give greater ownership of data back to citizens, letting people track how their identity is used, giving them the ability to select who they share data with, in what context, along with the power to revoke access," says Ricky Walker, chief technology officer for the public sector at digital transformation company Kainos.

"This would create transparency and build trust in the system, helping to encourage higher opt-in rates and adoption."

The new trust framework is scheduled to roll out in 2021. With more people set to use online services post COVID-19, many hope the government can learn from the past and ensure the right technology, processes and standards are in place to enable a new era of digital identity. Only then can it play a role in unlocking the UK's digital economy.

Policy Exchange 2020

1 in 5 people in the UK have no root anchor document, such as a passport or a driving licence

1bn people globally are recognised as lacking any form of digital ID

8% increase in identity fraud in the UK from 2017 to 2018

Matthew Horwood/Getty Images

VACCINES

Vaccine passports: are they the answer to pandemic recovery?

Documents identifying those who have been inoculated could help governments reopen after lockdown, but they also raise questions over privacy and patient rights

Daniel Thomas

With the rollout of mass vaccination programmes against coronavirus in a number of countries including the UK, many people are beginning to contemplate doing everyday things again, from going to the cinema to taking a holiday or attending a concert. However, with cases still high and worries about new variants emerging, businesses are increasingly likely to want proof their customers have had the jab and don't pose such a health risk to offer them these services.

Already, both Australian airline Qantas and UK cruise firm Saga have said their passengers will need to have been inoculated to travel with them in the near future. And London-based plumbing business Pimlico Plumbers says vaccination will be a contractual obligation for new and existing staff, although employment lawyers have raised concerns over how this would work in practice.

The question is how will people prove their vaccination status, particularly if it is requested multiple times a day in multiple different places. So-called vaccine passports are being touted as the most likely answer but how could this work in reality?

The benefits of a digital passport

The idea behind a digital vaccine passport is that people would download and present their medical records on their smartphones in an encrypted, yet verifiable, way.

Most countries currently issue proof of vaccination in the form of paper certificates, for example, a GP surgery will give travellers a paper booklet to prove they have had a yellow fever jab. But critics say these can be easily forged, are not universally recognised and a more practical digital alternative is needed.

Technology and healthcare companies from around the world are now working to make vaccine passports a reality. Take, for example, CommonPass, a health travel app being trialled by major airlines, such as United and Virgin Atlantic, and the World Economic Forum.

Users would be able to upload their vaccination records or COVID-19 test results into the app, which turns them into a uniquely generated "digital health certificate" in the form of a QR code. This can be shown to authorities without revealing sensitive identifying information, such as someone's name or address.

The need for shared standards

Then there is the Vaccination Credential Initiative, a coalition of organisations including the non-profit healthcare company Mayo Clinic, as well as technology firms Microsoft and Oracle, that is working to develop common technical standards to underpin such apps.

It follows a plea by the World Health Organization for open, interoperable standards, amid fears that countless individual passport apps will be created, making them unusable.

However, there are serious barriers that could stop passports getting off the ground. Firstly, no one knows how long the immunity provided by the new vaccines will last or whether they will stop people from transmitting the virus. If vaccines can't contain the crisis, then vaccine passports will serve little purpose.

Protecting patients' rights

Passports also pose "essential questions" about privacy and data protection because they depend on access to people's private medical records, says Dr Ana Beduschi at the University of Exeter Law School. This means policymakers are going to have to think carefully before they give tech firms unfettered access to patients' records.

There are ethical concerns too because passports "create a new distinction" between individuals based on their health status and can be used to determine the degree of freedoms and rights they may enjoy.

"Take the hypothetical scenario in which public authorities would require everyone to routinely display their health to access public and private spaces such as public transport, restaurants or churches," Beduschi explains.

"Such measures would restrict considerably the rights and freedoms of those who have the disease or did not receive a vaccine."

Some people may not be able to have the jab for health reasons, others may simply not want it. Then there are those who do not have smartphones or access to stable internet connections, all of whom could argue that not having a passport breaches their rights to equality and non-discrimination.

Is anonymity the answer?

Developers are alive to these issues and stress their apps are secure. Take the passport created by iProov, a UK biometrics startup, and cybersecurity firm Mvine, which is currently part of a government-funded trial.

Similar to CommonPass, medical professionals administering the vaccine would create an online certificate in the form of a QR code via the app, but they would also ask the vaccine recipient to have a selfie added to the certificate.

When the holder wanted to show the certificate, at a restaurant or venue for example, they would present the code and then verify their face against the attached image via the app.

> **Measures would restrict considerably the rights and freedoms of those who have the disease or did not receive a vaccine**

"The certificate does not need to include the name, address, NHS number or any other identifying information about the person; it is completely anonymous," says iProov founder and chief executive Andrew Bud. "It also doesn't discriminate against people based on the smartphone they own and there is a route for people who do not possess a smartphone, a card-based method."

However, Bud says it will ultimately be up to policymakers and health officials to address the legal, social and political questions around vaccine passports if a solution like this is to move forward.

Problems that seemed insurmountable at the start of the pandemic have been overcome and many believe this will be the case with barriers to vaccine passports.

Lucy Yang, community director of the COVID-19 Credentials Initiative (CCI), another group working on shared standards for passports, says coronavirus exposure notifications faced similar ethical and privacy barriers.

"Within a few months, more than 20 states in the US and 20 countries had adopted exposure-notification apps. If they achieved it, I don't see why we can't," she says.

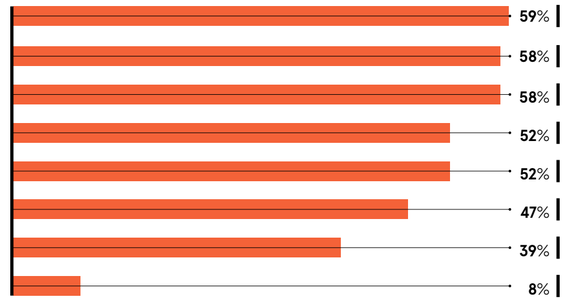
However, Yang explains, passports are unlikely to have as big an impact without shared standards and agreeing on them "won't happen overnight". In addition, while she thinks the technical challenges can be overcome, she's less sure about the other barriers.

"Hopefully CCI will launch a pilot in the next two to three months with multiple jurisdictions, then we will know better if it works. But the bigger challenge will be putting the right rules in place. Who should be issuing vaccine credentials in the first place and who should be verifying them?"

HOW BRITONS FEEL ABOUT THE COVID-19 VACCINE

IBM Security 2020

Percentage of UK adults who agree or strongly agree with the following statements:



SELF-SOVEREIGN IDENTITY

Taking control of your digital identity

Our personal data is fragmented online across a number of institutions and services, compromising its security and citizens' privacy. A new solution proposes putting the consumer back in control

Amelia Tait

Where are you? It's an easy question with one correct answer: you are where you are, whether that's at your desk, in bed or on a train. But the question becomes much harder to answer when we ask: where are you online?

You can probably count the digital accounts you use most frequently on your fingers: a ride-hailing service, a social media platform, a banking app. However, you need only look at your email inbox to realise how many services you've signed up for, the countless companies you've given your address, date of birth, mother's maiden name.

The truth is that on the internet, you're all over the place.

We have different digital identities for the different services we use and we're only ever one "what was the name of your first goldfish?" away from realising just how messy this can be. This system is known as centralised identity, where different organisations are responsible for keeping an abundance of people's data safe.

Over the past few years, a federated identity system has taken off, in which companies such as Facebook and Google allow you to log on to different platforms through their service. It is convenience at a cost because these tech giants can thenfollow you across the web, collecting data from your healthcare apps, shopping accounts or any platform you've used the "log in with Facebook" button for. Not only is this troubling in terms of your privacy, it is a goldmine for hackers.

Enter Self-Sovereign Identity (SSI), an enticing solution that promises to keep your data under your control. As Irra Ariella Khi, co-founder and chief executive of cybersecurity startup Zamna, puts it, with SSI you are "the king or queen of your identity". But even this new solution is not without its drawbacks.

What exactly is SSI?

SSI is an alternative digital identity model by which each user controls their verifiable credentials – tamper-proof electronic versions of physical credentials like a passport, permit or proof of address – and can selectively hand over bits of data to those who need them.

While SSI's proponents agree on its principles – it should be decentralised, user empowered, and everything must remain portable, private and, most importantly, secure – there is some debate over exactly how this can be achieved.

Many believe blockchain could be the answer, enabling each data attribute to be registered to a block on the decentralised chain that-businesses can access to obtain an individual's data without the need to store it themselves.

Many different entities are currently trialling SSI systems, from the Catalan government in Spain to an NHS hospital in Blackpool. Banks are also dipping their toes in the water, with Barclays previously exploring the benefits of SSI with specialist Evernym. "SSI has considerable potential when it comes to improving customer experience: users may be able to register with a single click, instead of having to fill out lengthy forms," according to Barclaycard's website.

> Self-sovereign identity has considerable potential when it comes to improving the customer experience

How can SSI benefit businesses?

SSI might be costly to implement, but could save businesses money in the long run. At present, companies receive hefty fines if customer data is lost or hacke, while maintaining security systems that prevent this is expensive. SSI both shifts the onus away from corporations and makes them less appealing to hackers.

Michael Shea, managing director of technology consultancy The Dingle Group, says SSI can also improve data quality, which will save on admin costs. "If the customer is able to present part of their credential, say their home address, because it's now in this cryptographic bundle that's been issued and verified, then nobody's entering any information on the keyboard," he explains. "It's done automatically, and so you eliminate the human-entry error or production mistake. There's huge value there."

He also notes that SSI won't just change how existing businesses operate, it can create new opportunities. He references Energy Web, a company that uses SSI to allow anyone to participate in the energy market.

"Traditionally, if you had solar panels on your house and you produced more power than you could use, it flowed back into the grid and your meter might run backwards. The grid operator cannot use it to balance the power on the grid because there are too many unknowns," explains Shea. SSI allows Energy Web to verify individuals and the equipment they use.

"They've created this sort of identity bundle that's all cryptographically signed, so you can become an active member of the power grid," he adds.

> SSI models are too often techies building for techies. When it comes down to it, if SSI is to be the panacea, then it has to cover everybody and everything

What problems does SSI pose?

Of course, problems arise when theory is turned into practice. Zamna's Khi notes there is an issue with SSI because it doesn't recognise what centralised institutions provide us with in return for our data.

"If you state the user is the most important person in this ecosystem, then we're ignoring the fact that the hard work of assessment and risk management, business processing and decision-making, and service providing actually doesn't happen on the user side," she says. "There are prices of admission to the services we as individuals want to have."

Zamna's co-founder Alex Gorelik warns that "technology by itself doesn't really solve anything" and that a rush to apply SSI can be directionless, with theorists not understanding how it can solve the problems faced by individual businesses.

Susan Morrow, head of research and development at identity data specialists Avoco Secure, has written about her doubts surrounding SSI. While in theory she supports giving users control of their data, she says SSI models in practice do not take human behaviour sufficiently into account.

"They're techies building for techies," she says. "When it comes down to it, if you want this to be the panacea, then it has to cover everybody and everything." In reality, many people don't have the smartphone or reliable internet access that a "wallet" system would rely on.

Questions also remain about the trust layer of SSI. Verified credentials are confirmed as cryptographically sound and untampered with, but Shea points out they do not prove whether a document was issued by a legitimate organisation. Khi has exposed such flaws, showing how easy it is to purchase a domain name using the title of a coronavirus-testing company. This means people could abuse the system, including, for example, where a border force requires travellers to have a negative COVID-19 test before they enter a country.

Identity custodians

A further issue is that if our digital identity remains totally decentralised, then there's no one we can call if everything goes wrong. There is therefore a need for identity custodians - individuals or entities we can rely on to help us recover our data. Some argue banks are a natural fit for the role, as we already trust them with our money and identities. Others, however, may prefer governments to take on the job.

Much remains to be resolved with SSI, but the coronavirus pandemic has accelerated interest. Shea says the landscape has shifted and more of his clients are focused on digital identity and SSI, with investment increasing. "It's getting a lot of attention," he says.

Perhaps controlling your own digital identity is just around the corner.

1000%
increase in digital identity revenue projected over the next 4 years

$1bn
annual revenue by 2024

88%
of this revenue will come from businesses paying a subscription to run these identity services

IBM Security 2020

Commercial feature

Digital identity is broken and it's time we fixed it

Digital fraudsters pose a huge threat to consumers and businesses alike, preying on online tractions and interactions, but keeping them away doesn't have to mean friction for users

Digital identity, as we currently know it, is broken and with the coronavirus pandemic accelerating the migration to online, fuelling a boom in internet fraud, the need to fix it is growing more urgent.

In the physical world, we identify people instinctively because of their characteristics: their face, voice, body language and the way they walk. Online, however, it's much harder to prove identity and easier for fraudsters to pretend they're someone they're not.

Authenticating people when conducting online transactions, or other interactions that require user verification, is therefore vital to preventing fraud.

However, having to authenticate ourselves regularly online creates friction that turns many customers away, creating a Catch-22 for businesses. Research by Decibel found that seven in ten customers abandon purchases because of a bad user experience. To improve digital identity processes, we have to understand where they went wrong. The answer is they simply tried to replicate physical ID processes in a digital way.

"If people can now get everything they need online, what influences loyalty? It's predominantly the user experience, but security and privacy are also becoming more important," says Amir Nooriala, chief commercial officer at Callsign, whose artificial intelligence-based identity and authentication solutions allow customers to interact safely online, with minimal friction, while ensuring bad actors are blocked to protect customers' identities.

"Fraud needs volume to hide itself in and that volume is now online. Every company should be asking how they can ensure they have the best online experience without opening the gates to fraud. You do it with passive technology that collects multiple different data signals without affecting user experience, giving the best of both worlds."

> Every company should be asking how they can ensure they have the best online experience without opening the gates to fraud

Passively collecting information, while sustaining an optimal user experience, means thinking about digital identity in purely digital, not digitalised, terms. It requires portability of identity across both devices and channels, including web, mobile and open banking.

By analysing the thousands of datapoints across device, location and behaviour, Callsign can confirm in real time whether users' behaviours fit their normal pattern. If they do, they can get on in a frictionless way, but when they don't, or malicious activity is detected, Callsign introduces further tests, avoiding a rules-based approach that is easily replicated by bad actors. This allows users to get on with their digital lives, while businesses improve customer engagement and productivity, and reduce fraud risks.

Placing identity at the core of their business is the digital version of putting the customer first. It helps ensure smooth online experiences and transactions, but also secure, privacy-preserving experiences, and getting this right drives customer loyalty.

"We're completely rethinking digital identity," says Nooriala. "Utilising artificial intelligence and machine-learning models, we use real-time data to confirm if your device is recognised and that it's free from malware, alongside behavioural traits such as how you type or how you swipe, the pressure your finger places on the screen and the angle you hold your phone, as well as your location."

"With all these passive data signals, we secure online transactions and massively reduce both digital fraud and friction in the user experience. And it's all done in a privacy-preserving manner. Unlike most approaches, which require constant surveillance, we put privacy at the centre. By only collecting data at each transaction and analysing against previous behaviour, not individuals themselves, we know who you are without knowing who you are."

While other companies ask users to verify their identity again and again, and rely on physical authentication checks, Callsign's passive approach puts identity at the heart of every transaction, facilitating a more holistic and intelligent view of the customer. The more people move online, the more important this will become. Organisations that succeed digitally will be those that recognise identity is part of every online interaction.

For more information please visit callsign.com

callsign

Jonathan Knowles via Getty Images

DEEPFAKES

Deepfaking it: the new cybersecurity frontier

From impersonating a top executive to opening money-laundering bank accounts, deepfake fraud is becoming a growing problem and poses real challenges

Emma Woollacott

A few weeks ago, on a routine company video call, one of the tech groups decided to prank the boss and five of them turned up looking like him.

"It was very spooky. They used a publicity still of me and the person in the publicity still was blinking, moving his head, smiling, talking, saying things I don't say, but it was me," Andrew Bud, chief executive of biometric authentication provider iProov, recalls.

Over the past couple of years, deepfakes – manipulated videos or audio recordings that appear to show individuals doing or saying things they never did or said – have started to emerge. Most feature celebrities or political figures, with some created purely for amusement value and others vehicles for misinformation.

The deepfake threat to businesses

However, new types of deepfake have now entered the frame with the aim of committing fraud. Indeed, the use of deepfake video and audio technologies could become a major cyberthreat to businesses within the next couple of years, cyber-risk analytics firm CyberCube warns in a recent report.

"Imagine a scenario in which a video of Elon Musk giving insider trading tips goes viral, only it's not the real Elon Musk. Or a politician announces a new policy in a video clip, but once again it's not real," says Darren Thomson, head of cybersecurity strategy at CyberCube.

"We've already seen these deepfake videos used in political campaigns; it's only a matter of time before criminals apply the same technique to businesses and wealthy private individuals. It could be as simple as a faked voicemail from a senior manager instructing staff to make a fraudulent payment or move funds to an account set up by a hacker."

In fact, such attacks are already starting to occur. In one high-profile example in 2019, fraudsters used voice-generating artificial intelligence software to fake a call from the chief executive of a German firm to his opposite number at a UK subsidiary. Fooled, the UK chief executive duly authorised a payment of $243,000 to the scammers.

"What we're seeing is these kinds of attacks being used more and more. They're not overly sophisticated, but the amount of money they're trying to swindle is quite high," says Bharat Mistry, technical director, UK and Ireland, at Trend Micro.

"I was with a customer in the UK and he was telling me he'd received a voicemail, and it was the chief information officer asking him to do something. Yet he knew the CIO of the organisation was on holiday and would never have phoned. There was no distinguishing factor, so you can see how clever it is."

Attacks such as this follow the same pattern as traditional business email compromise scams, but with vastly more sophistication.

"We've seen all these cloud technologies, things like analytics, machine-learning and artificial intelligence, and deepfakes are just an extension of that technology, using the tech in an abusive manner," says Mistry.

Creating fraudulent accounts

Another emerging type of deepfake fraud is the fraudulent creation of accounts, whether they are bank accounts, foreign exchange dealing accounts or share dealing accounts. These can be used by organised crime for the purposes of money laundering. And with the advent of the coronavirus pandemic, what was previously a gradual shift to remote account creation has now been massively accelerated, along with the potential for fraud.

> **It's only a matter of time before criminals use deepfake videos on businesses and wealthy private individuals**

Setting up an account remotely generally involves a two-step process: first, providing a scan of an identity document and then presenting a selfie. The selfie is often generated by asking the applicant to record a video in which they recite words or numbers, or perhaps through a short video interview with an agent.

"It's obviously been a good way of protecting against fraud up until now, but now the fraudsters can deepfake themselves to look like the innocent victim," says Bud.

"They may have stolen or copied the documents of an innocent victim from some source, and then all they need to do is deepfake the victim's face onto their face and conduct the interview with the agent, and the agent will be never the wiser."

In a report late last year, identity verification firm Jumio found selfie-based fraud rates were five times higher than ID-based fraud and particularly prevalent where users are able to upload their own ID images. This means fraudsters can manipulate a legitimate ID or use an image of an ID found on the dark web or from a Google Images search.

Financial institutions are awakening to the risk. In a survey for iProov, three quarters of cybersecurity experts in the financial sector said they were concerned about deepfake fraud and nearly two-thirds said they expected the threat to get worse.

"Banks like ING, Rabobank in the Netherlands, Standard Bank in South Africa and the government of Singapore, which is supplying the financial services industry, these are all aware of the threat of deepfakes and are taking proactive measures," says Bud.

However, only 28 per cent of survey respondents said they'd put plans in place to protect against deepfakes, with 41 per cent planning to do so in the next two years.

With another poll of banking customers revealing most were unconcerned about deepfake fraud, introducing extra security measures can be problematic.

"There's a big difference between how much cybersecurity experts think people care and how much they do care, and that turns into a problem as soon as they try to implement intrusive measures," says Bud.

"There is a risk that if they protect against deepfakes in ways that impact the customer experience, it will be immediately resisted."

The first line of defence against impersonation attacks, says Mistry, is to make sure all standard security procedures are implemented and to build in automatic checks.

"If they're asking for a money transfer or to change something or to amend something on a document, then it should be verified through another channel," he says.

Financial institutions, meanwhile, are turning to more sophisticated methods of detecting deepfakes.

Passive liveness detection uses algorithms to detect signs in an image that it's not genuine by examining textures, edges and the like.

Increasingly, though, active detection is being used, introducing unpredictable information the deepfaker can't predict and therefore can't effectively spoof.

"What we do is illuminate the subject; we use the screen of the person's device to illuminate them with a rapidly changing sequence of colours," says Bud.

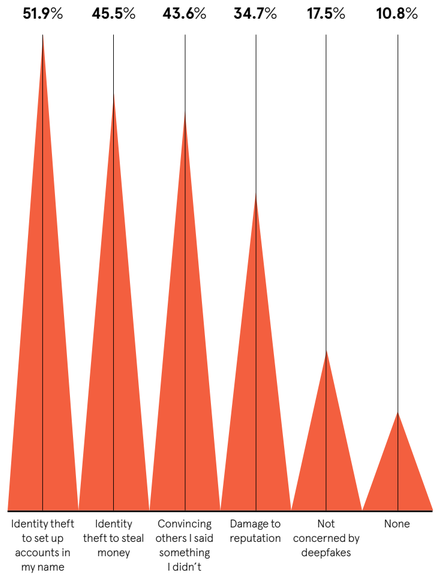
"Then we stream the video of their face back to our servers and analyse the way the light reflects from their face and the sequence of colours reflected on their face. This is is an unpredictable element that it's difficult for a deepfake to replicate effectively."

What's clear is the use of deepfakes for fraud is an escalating risk and over the coming years the arms race between fraudsters and security professionals will only increase.

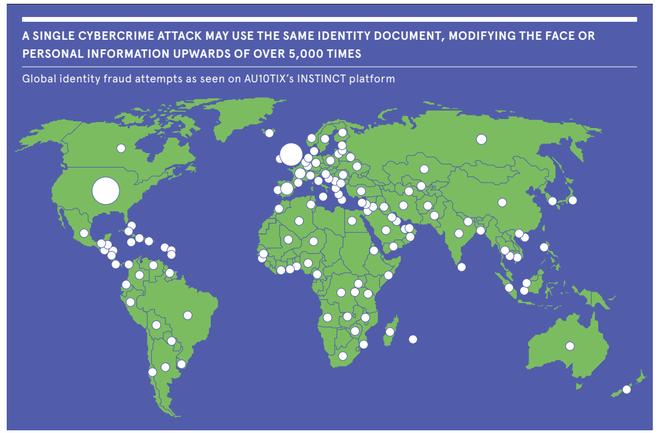
"At the moment it's in its infancy; a lot of cybercriminals are still after using ransomware or business email compromise. But as these channels start to dry up and people cotton on, they're going to move on to deepfakes more and more. At the moment, the only limiting factor is the technology," Mistry concludes.

THE THREAT OF DEEPFAKES iProov 2020

What worries US consumers about deepfake technology?



Commercial feature



The danger identity fraud poses and what companies can do

A more adaptive approach to verifying identities that eliminates industry, organisational and data silos can allow companies to tackle fraud more intelligently

Enterprises have for too long taken a siloed approach to digital identity processes. Different data structures are owned by different departments, who often have contrasting, even competing, objectives when it comes to onboarding and managing users. The compliance group examines personal data in light of various regulations while the risk group looks to reduce fraud losses, and it's all independent of the product management and customer support departments.

Such fragmentation is creating friction-filled experiences and consumer frustration, while national and international silos at a data level are also inhibiting companies from learning from identity insights outside of their own organisation. Privacy concerns have understandably fuelled data protectionism, however new tech advancements now mean encrypted data signals can be shared to bolster fraud defences without any identifiable user information being shared.

The business challenge of a fragmented digital identity

Fraudsters know how debilitating silos can be, which is why they not only seek to exploit them in the businesses they attack but also avoid them in their own activities by embracing networks. To combat synthetic fraud, which already accounts for 15 per cent of credit card losses, according to Experian, and is the fastest growing type of financial crime, organisations must partly learn from the fraudsters themselves.

"The way cybercriminals behave is not siloed at all, it's networked, so how do we fight them in the same way? We're learning that businesses have to be adaptive and collaborative in order to compete," says Carey O'Connor Kolaja, CEO at identity management and intelligence company AU10TIX, whose solutions link physical and digital identities so companies and consumers can confidently connect.

"Identity has traditionally been thought about in terms of what needs to be known to verify access to something particular. If I want to buy alcohol, I have to show my ID but the seller only needs to verify I'm over the legal drinking age. If I want to get a loan from a bank, there's a lot more about me and my financial suitability that must be shared.

"Over time, identity is not just a government issued ID or a digital footprint – it's an accumulation of information that describes you and your behaviours, meaning identity becomes much bigger than we ever realised, as do the opportunities for cybercriminals. We're seeing fraud attacks from the most unexpected places with PII not necessarily acquired from a full account takeover but through skimming small bits of information from unsuspecting sources."

The unified fight against synthetic fraud

AU10TIX's has transformed from developing technology identity verification for border control and airport security to identity intelligence that supports customer due diligence and onboarding for brands like Google, PayPal and Uber. Its unique heritage gives it a strong edge in understanding what happens across the physical and digital divide, and has allowed it to launch INSTINCT, a synthetic fraud detection solution that is able to verify the authenticity of an identity through data signals alone. This will enable a global network of data signals that aids companies in fighting fraud together.

"When you start to look at synthetic fraud over a continuum, you can really unearth where the perpetrators are," says O'Connor Kolaja. "We're catching 50 synthetic identity attacks in any one company on a given day. Most importantly, we're able to not only stop synthetic fraud in one network or 'closed garden', but safely share the intelligence with other organisations around the world so they can prevent the same attack from happening again – continuously updating a synthetic identity watch list.

"Covid-19 has created an environment where people are concerned more about cyberattacks than terrorist attacks. It has forced identity protection to the forefront of our minds and amplified the need to understand how, through technology, our identities and behaviour can be used to equalise and authenticate our access to all life's experiences. We have to grasp this opportunity to accelerate unification and adaptive identity processes, advancing our progress to a more secure and inclusive world."

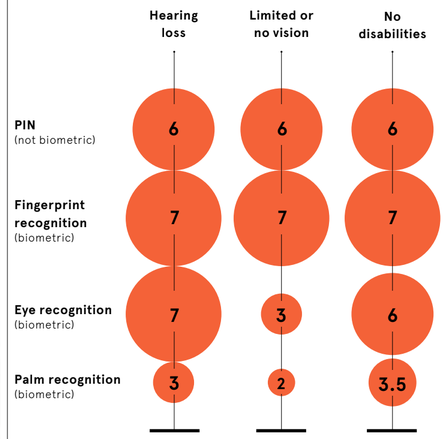
For more information, visit www.AU10TIX.com

AU10TIX
IDENTITY INTELLIGENCE

MoMo Productions/Via Getty Images

WHICH BIOMETRIC TECHNOLOGIES ARE THE MOST ACCESSIBLE?

Respondents from three groups – those with hearing loss, those with limited or no vision and those with no disabilities – rated four authentication methods according to the statement "this system is easy to use". 1 is strongly disagree, 7 is strongly agree.



Mitre 2019

ACCESSIBILITY

Ensuring biometrics work for everyone

Too often products are designed without taking people with disabilities into account; with security technologies, the limited usability of some biometrics could have serious consequences

Abby Young-Powell

Biometric technologies, such as fingerprint identification, retina scanning or voice recognition, can improve the experience, security and usability of electronic devices for many. All too often, however, those with disabilities are overlooked in the design process.

People with a loss of dexterity may have difficulty using biometric fingerprint technology, someone with a voice tremor could struggle with voice identification and blind people may find facial recognition does not work for them.

If people with disabilities are forced to discard biometric security innovations they could be less secure online. "Then people are less able to engage in a digital lifestyle," says Robin Christopherson, head of digital inclusion at AbilityNet. "This has a huge impact and leads to massive disenfranchisement." So how can biometrics be made more accessible?

There is limited research into the usability of biometrics for people with disabilities. However, a recent study by US not-for-profit organisation MITRE found biometrics that required dynamic device positioning, such as holding a phone or laptop in a certain place in relation to your face, lack usability for people with limited or no vision, according to researcher and senior human factors engineer Ronna ten Brink.

In fact, a large number of us could be affected if digital identity technologies are not accessible, especially as we get older. Chris Millington, managing director of Emporia Telecom, which has been making simplified smartphone features for retirees, says: "For many of us there is disability, such as hearing loss, sight loss and loss of dexterity, in the ageing process."

Becca Scollan, senior human factors engineer at the Mitre Corporation alongside ten Brink, agrees. "You might not have a disability now, but you could injure yourself," she says. "Plus we all age, which brings on greater potential for having a disability."

Legislation, such as the Americans with Disabilities Act or the Equality Act in the UK, exists to prevent discrimination against disabled people. However, Christopherson says it is not always enforced.

> **Accessible products are not just easier for disabled people, they're easier for everyone to use**

It's not enough to strive to meet minimum requirements either, says Matt Webb, group head of digital at LAB Group, who has decades of experience working with technology providers. At the moment, too many tech developers are working towards the lowest possible bar, he says. "So if someone can't use a fingerprint scanner, just give them a password," he says. "That kind of approach is a worry."

There are many reasons technology companies should want to make biometric authentication accessible, without being forced to do so. "It's good for your brand and you've got the purple pound," says Christopherson. "Accessible products are not just easier for disabled people, they're easier for everyone to use. Plus disabled users are massive advocates for tech, so you have a really invested audience."

Technology companies should be supported in the process. "It's about supporting organisations [to create accessible products]," according to Keir Haines, senior product designer at Designability, a charity that enables disabled people to live with greater independence.

How can tech providers enrol disabled people in the development process? "It's about building on a more diverse framework at the beginning of the design process," says Dr Louise Hickman, senior research officer at the Ada Lovelace Institute. Accessibility should be woven in right from the start and not considered as an afterthought, she says.

Having more diverse teams would also help. "Ideally in the development team, but definitely in the user testing," adds Christopherson.

Another solution is giving users a choice when it comes to biometric accessibility and security. One of the recommendations from the MITRE report is to offer more than one biometric option for users. "Biometrics best practice is to offer a range of alternatives so people can choose from a range of options," says ten Brink. Users can then select the biometric option that suits them best.

Biometrics have the potential to improve the lives of people with disabilities. Christopherson says that, as a blind person, he struggles to use CAPTCHA, which relies on images to determine whether a user is human. "I'm often told I'm a robot," he says. "But if CAPTCHA challenges were replaced by biometrics that would help a lot. For disabled people, biometrics represent a huge opportunity."

Voice recognition can be a game-changer for people with physical disabilities or sight loss, while biometric logins, such as fingerprint, face or iris authentication, can work for people with physical disabilities or those with dyslexia who might struggle to remember passwords.

"Accessing services in person can have additional challenges when you have a disability, so anything that allows you more access to services from wherever you are in the world is something that helps people with disabilities," says ten Brink.

But technology providers need to keep disabled people in mind when developing biometric innovations. It's important to make products inclusive now. "If we don't, then the only people who are going to be left using passwords are the disabled because they've not been catered for," says LAB Group's Webb.

It's not just people with disabilities who will benefit from more usable products. "It's in everyone's best interests to design with people with disabilities in mind because you're generally making your products better," Scollan at Mitre concludes.

Commercial feature

Self-sovereign: the new dawn of digital identity in travel

Giving identity storage and control back to the passenger is the next step, but how can organisations ensure customer relationships are not lost?

Organisations are spending huge sums in efforts to protect sensitive identity data and meet consumer demand for both next-level data privacy and frictionless experiences where a secure digital ID is used to access interconnected services.

The self-sovereign identity (SSI) approach continues to gain traction, recentring the notion of identity around the individual. Put simply, the individual owns and controls access to their identity data, and can use it to access goods and services from different organisations. But with identity data moving out of the corporate environment and into the hands of the consumer, how can organisations ensure their customer relationships remain intact?

Here are four considerations to bear in mind:

> **Travel companies have become a hotbed of personal identity data**

4.4bn
individual passenger flights globally in 2019

8bn+
individual identity transactions involving sensitive personal data including biometrics

10k+ years
annually spent on processing and verifying identity across global air travel

Airportwatch

1. Identity data is dangerous

Data is constantly under attack. Identity, credit and cyberfraud costs an estimated £190 billion a year in the UK alone, according to think tank the Royal United Services Institute.

At the same time, stricter privacy regulations heighten the risk of huge financial and reputational loss. For example, 9.4 million Cathay Pacific passengers were impacted in aviation's largest known data breach, leading to a government inquiry and a £500,000 fine.

As the requirements for identity data increase, which in travel now include other sensitive data such as biometrics, current health status and visas, travel companies have become a hot bed of personal identity data.

Given the coronavirus pandemic, there is the additional challenge of inextricably linking a customer's health status to a secure verified identity at the point of travel.

Organisations need an approach that allows them to set up a singular, persistent verified digital identity for each customer. They must also be able to orchestrate and configure the use of that identity while not storing or controlling the data themselves.

To enable this, Zamna has created a unique decentralised approach it calls Identity Rails. Similar to how open banking has transformed financial services, Zamna's Identity Rails are set to transform the way in which identity data is managed, stored, shared, connected and controlled between organisations and individuals.

"The strength in our approach lies in how companies can create valuable partnerships within their commercial ecosystems with verified identities at the centre," says Zamna chief executive Irra Ariella Khi. "Giving identity storage and control back to the customer, without losing them to your competitor, is paramount; our Identity Rails infrastructure solves this."

2. Bad data, bad decisions

Quality data is at the heart of every business decision, from assessing risk and allowing access to services, to crafting personalised marketing campaigns at scale. But how accurate, and how verifiable, is identity data flowing through these systems? The truth is it's neither, yet.

"The foundation of identity data needs to change. You need a way to validate whether it is correct and establish if it's been seen before, while also removing the need to control or store," says Khi.

"Zamna enables organisations to create super smart verification 'signals' that allow recognition and validation of identity data previously seen but not stored. From this, clients can remove the need to store sensitive data, aggregate verifications and work towards cleaning up identity data at scale. A single version of truth is the starting point."

With airports empty due to the pandemic, travel companies are rapidly transforming the way in which they can service and monetise passengers

3. Trust and privacy are everything

Trust is a huge challenge for organisations. Millions are invested in tools to trust that people are who they say they are and yet identity fraud is at an all-time high, says UK fraud prevention service Cifas. Given low adoption rates and privacy challenges, it is evident there's no silver bullet consumer app that will single handedly solve digital identity at scale. So how can organisations create trust and privacy at scale?

> **Self-sovereign gives identity storage and control to the customer, but not losing them to your competitor is paramount; our Identity Rails infrastructure solves this**

"We use permissioned distributed ledger technology to harness the power of a curated network at scale and in real time. The immutability of this type of system means once a verification event has happened it can never be altered or reversed, but it can be recalled," explains Khi. "From this base, companies can enable their customers to create persistent identities secured by both biographic and biometric identity attributes."

"Putting secure identity at the centre of your business, together with trust, extends new commercial opportunities and business models."

Airlines are exploring this to solve the challenge of verifying and servicing vast numbers of passengers to enable frictionless travel. Zamna has been instrumental in the development of the International Air Transport Association's One ID framework, which is set to harmonise the way identity is managed across a notoriously fragmented travel ecosystem.

4. Connecting the dots

The dream for the post-pandemic traveller is a joined-up experience, where they can control and prove their identity only once before even booking a trip, and seamlessly share this with airline, rental car and hotel systems. But allowing identity data, and the trust in that data, to flow freely through the travel ecosystem in this way has, until now, been an insurmountable problem, exacerbated further by increasing data privacy concerns.

"Our Identity Rails are the next generation of corporate infrastructure for individuals and organisations to trust, orchestrate and control identity data without the limitations of existing self-sovereign identity technology. Organisations can put their customers back in control, but maintain operational and commercial value," says Khi.

The development of next-generation privacy and security strategies is now a non-negotiable for organisations dealing with identity data. Tools that orchestrate identity within an organisation, and with chosen commercial partners, while moving storage and control of this valuable, yet dangerous, data to the hands of the customer are where we are heading.

We've already seen the financial services industry move to the open banking framework to enable easy exchange of financial data transactions. Zamna believes its Identity Rails are the future for securely managing and orchestrating identity across organisations, and it has the travel ecosystem in its sights. Solving identity in travel is the holy grail. If this is Zamna's starting point, it may be the most important company in digital identity that you've never heard of.

For more information visit zamna.com

Zamna.

AUTHENTICATION

Holding customers accountable for authentication

As banks and other financial institutions look for improved ways to authenticate transfers and transactions, can they ever shift the onus of fraud risk to customers or should the focus switch to education?

Jonathan Weinberg

In a world where transaction fraud and online scams are more sophisticated than ever, banks and financial institutions face hefty bills for losses when customers fall prey to criminals.

Due to a mix of legal obligations and voluntary codes, stolen money is usually refunded in full, but with the number of such crimes on the rise, is this sustainable?

New, more secure authentication solutions to prevent fraud and theft in the first place are now coming online, but if the human factor can't be planned for, could we ever see customers bearing more of the risk profile?

Faced with everything from traditional passwords, two-factor authentication and one-time password codes sent by text, to the likes of voice recognition, face recognition and fingerprint scanning, it's easy to see why people get confused or become frightened about using authentication.

Such wide-ranging techniques are one reason why Nick Maynard, lead analyst at Juniper Research, doesn't think a shift in onus is likely. "We believe it is unlikely banks will be able to discriminate against customers who do not use certain technologies, given regulatory constraints.

"Banks will continue to introduce authentication technologies and encourage their use, but directly passing on risk concerns is unlikely to be something a regulator would consider permitting or the bank would want to do, given the negative reception such a move would generate."

Andrew Shikiar, executive director at FIDO Alliance, a global consortium working on the creation of open standards for simpler, stronger user authentication, agrees. "The banking industry invests huge proportions of its IT budgets to protect its customers. Unfortunately, bank and IT solutions are largely helpless on their own against one of the biggest threats that people face: social engineering. These attacks are often successful due to the fact that the point of failure is ultimately human," he says.

"Introducing strong authentication without frustrating customers will prove to be a competitive advantage for the banks that get it right. It is a major selling point to any customer that cares about their money or is fed up with increasingly convoluted processes getting in their way of simply accessing financial services."

Many experts advocate the need for far more education among consumers on all forms of authentication by the banks and financial institutions.

This could be especially important given future authentication ideas include a greater level of biometrics, document-centric identity proof, government-issued IDs with a corroborating live selfie, automated risk-management tools, device authentication and geolocation.

Another advance could be continuous behavioural biometrics, as explained by Gus Tomlinson, general manager at identity management, location intelligence and fraud prevention company GBG. "This is all about how we type, how we hold our phones and even our speech patterns. This is the hardest thing for fraudsters to try and do, and will be the best customer experience for users without compromising their security at all," she says.

"In the event of suspicious activity, real-time alerts are sent to support the customer's authentication process, eliminating the ability for fraudsters to hijack this process."

Craig McClure, director of relationship management for Chargebacks911 and Fi911, also believes education is critical. "Banks have a duty to look after their customers' money. To get customers to move to new and more secure ways of paying requires patience, education and reassurance," he says, "We can never expect customers to be responsible for fraud unless they have acted with gross negligence."

One area where education could now be vital is amid the growing use of multi-factor authentication techniques. With passwords and texts seen as weak links, banks and other financial institutions now use two or three levels of authentication for making transfers or payments.

Indeed, this year sees the UK rollout of strong customer authentication (SCA), part of the open banking European Union payment services directive PSD2. It is due to go fully live from September, regulated through the UK's Financial Conduct Authority, to ensure payment service providers, gateways, emerchants and technology providers have more robust payment processing security techniques.

Industry body UK Finance describes it as "a new set of rules that will change how you confirm your identity when making purchases online".

Three independent factors are featured, with a minimum of two used: something the user knows (passwords and security questions), something the user possesses (phone, token or card reader) and something unique to the user (biometrics).

But Daniel Cohen, chief product officer for anti-fraud at RSA Security, believes the UK faces a clash of regulations between the General Data Protection Regulation (GDPR) and PSD2. He explains: "The European Banking Authority won't accept commonly used SMS as a 'strong authentication' factor, so banks must add a second layer of behavioural biometrics, for example voice, keystroke or signature dynamics.

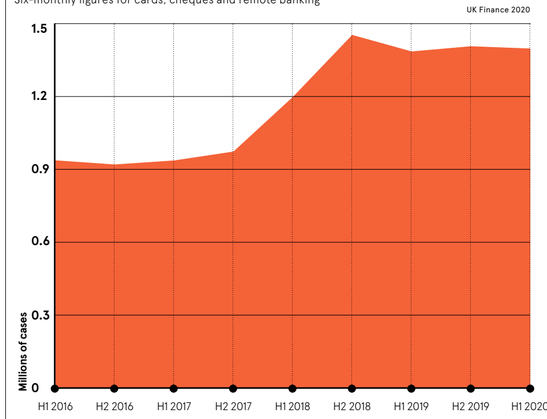
"Under GDPR, behavioural biometric data requires end-user consent. But what if consent is not provided? Banks cannot then authenticate the user in line with PSD2."

However, Niamh Muldoon, global data protection officer at OneLogin, argues SCA could be what marks the beginning of a shift in risk profile. "I believe SCA is a foundational step made by the financial and banking industry to transfer the responsibility and accountability of protecting their payment cards on to individuals," she says.

"With it, the industry has enabled individuals to make informed risk-based decisions. Now individuals need to stay conscious and aware, choosing to only use service providers that protect their finances and identity with strong authentication or multi-factor authentication."

CASES OF UNAUTHORISED FRAUDULENT TRANSACTIONS IN THE UK

Six-monthly figures for cards, cheques and remote banking



> **Introducing strong authentication without frustrating customers will be a competitive advantage for those that get it right**

Andrey_Popov via Shutterstock

OPINION

'We should be creating digital identity security that is not elitist and anyone can navigate'

We live double lives: we live a life in the physical world and we live a life in the digital world.

The shift towards which world we spend more time in began long before coronavirus, although the pandemic has certainly acted as a catalyst. The consumerisation of IT means that from the day we're born until the day we die, we spend increasing amounts of time in the digital world.

It's not unusual for expecting parents to make social media accounts for their child while they are still in the womb, creating a digital footprint before they have taken their first breath.

Toddlers are performing digital identity authentication to log on to Disney+, selecting the character chosen to represent their account to give access to the app.

At school, children log in to computers with QR codes or during lockdown they log in to Google Classroom from home with a username and password.

As we go through life, we create and open more and more digital accounts, for healthcare, work, school, socialising, shopping, government. They keep accruing and accruing and somehow it's deemed the primary credential method for authenticating these hundreds of accounts is our brain.

This would be perfectly tenable if we only had a couple of accounts and a couple of passwords, but we have hundreds. We're told they should all be unique and then we're instructed not to write them down. Our brain, then, becomes an impractical storage solution.

In our physical life, it's relatively easy to prove our identity. Being present means your identity can be checked against your government-issued ID. In our digital life, proving identity is more complex.

Digital identity is a combination of digital attributes and activities. Attributes include biometrics, email address, date of birth, bank details and login credentials. Activities include purchase history, geotagging, likes, comments, photos and shares on social sites. Any of these, or a combination of them, can function as a means for verifying digital identity.

According to MarketsandMarkets, the post-COVID global identity verification market size is expected to grow from $7.6 billion in 2020 to $15.8 billion by 2025, at a compound annual growth rate, or CAGR, of 15.6 per cent.

Market growth can be attributed to surge in digitalisation initiatives or, as mentioned, a shift to mainly living our digital lives, regulation and compliance requirements, and adapting to a post-COVID world.

Growth in digital identity verification is inevitable, but what isn't is that it will be done properly. We should be creating digital identity security that is not elitist and anyone can navigate, regardless of age, cognitive ability, disability or any other factor. We need a solution spanning our entire life and an interface which works to explain things in terms that can be understood wherever we are in life.

It must be robust and it must interface with security and privacy controls on your behalf. More complicated still, this solution needs to work across borders, to enjoy global trust, while remaining compliant with security and privacy regulations around the world.

Of course, it also needs to work at the speed of bits and bytes. An entity is going to have to earn trust to do this successfully.

Some industry analysts have predicted it will take more than a decade to secure this intermediary that covers our entire digital lifespan. If market growth predictions are to be believed, we may see a host of digital identity verification solutions coming to fruition before we reach that holy grail. The industry loves a challenge though and, if there's money to be made in solving a security problem on a global scale, it won't stop until it succeeds.

Eleanor Dallaway
Editorial director
Infosecurity Magazine

www.infosecurity-magazine.com

Commercial feature

Why the UK needs a 360-degree approach to digital identity

With coronavirus driving businesses and consumers online, it has never been more important to secure customer trust through digital identity

The debate over digital identity has taken on a new urgency with the surge in online transactions fuelled by the coronavirus pandemic. Businesses are rushing to adopt a digital model much sooner than many anticipated, while consumer reliance on technology to access everyday services has never been greater.

Securing customer trust is paramount as one in five consumers and two thirds of businesses were subject to identity fraud last year.

However, many businesses remain in the dark about implementing digital identity; some balk at the investment while others are wary of disrupting the customer experience.

This is particularly evident in new businesses. The reason? If you're a new business, the most important thing is getting people through the front door and focusing on immediate growth above future cost-savings.

The same is true for the retailers currently moving their businesses online. Their priority is quickly establishing a way to stay up and running during the pandemic – which could leave them exposed to fraud.

ONE IN FIVE CONSUMERS WERE AFFECTED BY IDENTITY FRAUD IN 2020

47% of consumers opened an online shopping account this year

28% of organisations worry they still tolerate 'high' or 'extreme' levels of fraud

1 in 3 businesses say COVID 19 has made them more worried about fraud

1/3 of over 75s opened a new online account in 2020

81% of businesses believe identity verification can be a strategic differentiator

Overcoming the trust gap

There are multiple ways to raise awareness among businesses of the importance of digital identity. One is the introduction of laws that regulate identity verification for individuals in the same way they do for banks.

The other is to take the lead from other countries, which have a strong digital identity infrastructure in place that can be applied across different sectors. For businesses, this template removes the cost and complexity associated with having to source different vendors to build a 360-degree digital identity solution and they know the user's identity is trusted.

For individuals, having one digital identity they manage themselves removes the headache of sourcing multiple forms of ID to access different services, and ensures an acceptable level of friction for customers during transactions.

This also helps overcome the trust gap that exists between consumers and businesses, which is exacerbated by almost daily headlines detailing the latest data breach.

So, while there is a tension around who is responsible for the consumer's personal data, the goal is to see a combination of technology and infrastructure that allows individuals to take control of their digital identity with greater transparency into where their data is being used, and as a result, greater control and responsibility.

Fragmented identity market

The problem is currently the concept of digital identity is incredibly fragmented in the UK. Take, the property sector. Anyone who has ever bought or sold a house will know they have to have their identity verified on multiple occasions by all the different parties involved. However, the same problem exists in many sectors.

Organisations are also offered fragmented off-the-shelf identity and anti-fraud offerings, based on the methods of least resistance. Much of this is because currently "who we are" is categorised in four different ways.

The first is how you're labelled: your name, address, date of birth. Then it's what you have: documents such as a driver's licence or passport, or your mobile phone. Then biometrics: unique identifiers such as your fingerprint, eyes or voice. The last one is your behaviour: how you move, your facial features, or how you interact with your devices.

Solutions built around these different components exist independently in the market, but are capable of only serving to prove parts of your identity. But unless businesses can layer those four things, they will lack the necessary context to be able to trust the identity they're dealing with.

360-degree approach to digital identity

Organisations need a 360-degree approach to digital identity that incorporates elements of those four different touchpoints. This means a connected, contextual identity engine, personalised for the customer. For the retailer this means layered checks to ensure the person on the other side of the computer screen is who they say they are.

We need a combination of technology, education and appropriate legislation from the government. Digital identity will be the foundation upon which our future economy is built. With COVID-19 accelerating the shift to digital, and with thousands of new online accounts being opened every day, digital identity should be a strategic imperative for all businesses.

For more information please visit www.gbgplc.com

GBG

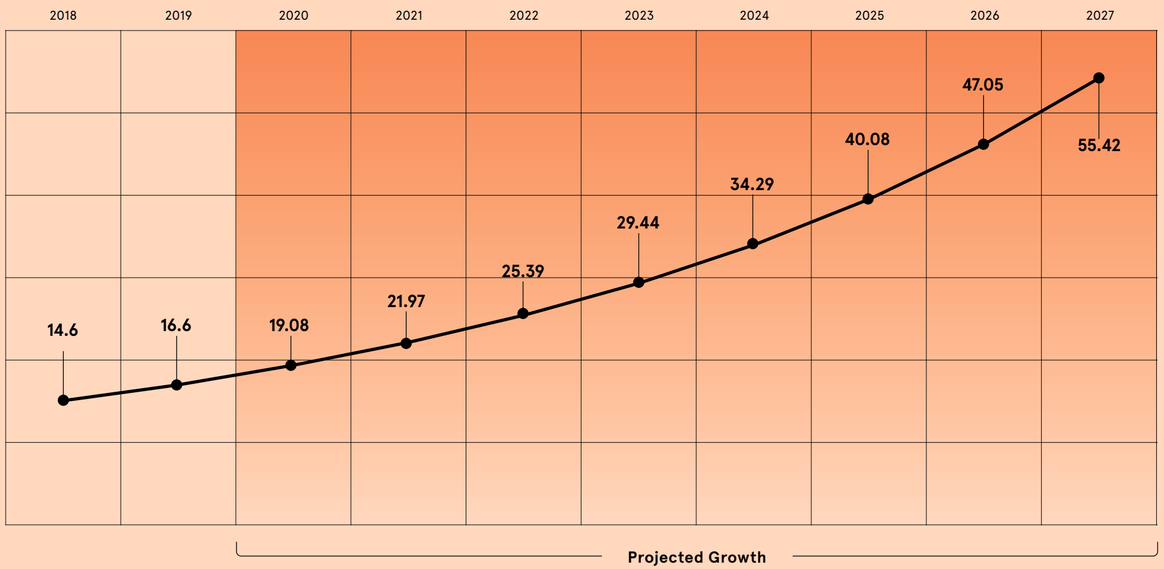
THE RISE OF **BIOMETRICS**

As people and businesses begin to understand the limitations of passwords, they are increasingly turning to biometrics to log in to services and authenticate users

THE BIOMETRIC TECHNOLOGIES INDUSTRY IS BOOMING

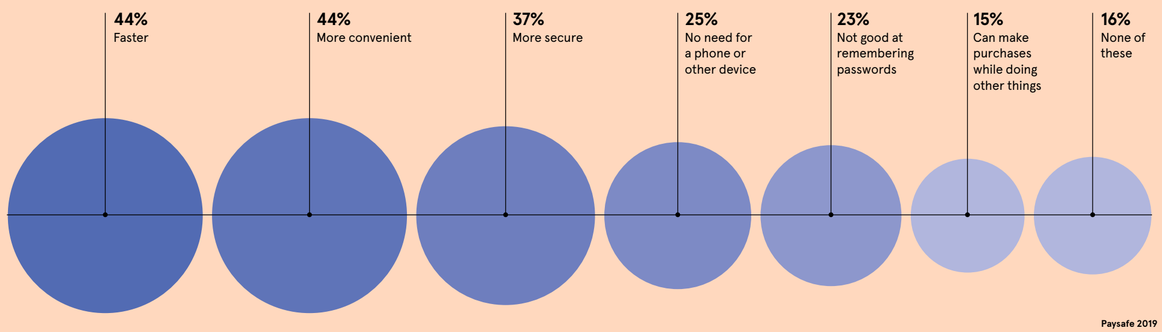
Global biometric technologies market revenue, in billion US dollars

The Insight Partners 2019



THE ADVANTAGES OF USING BIOMETRICS

The reasons why consumers in North America and Europe think biometrics have an advantage over other authentication methods

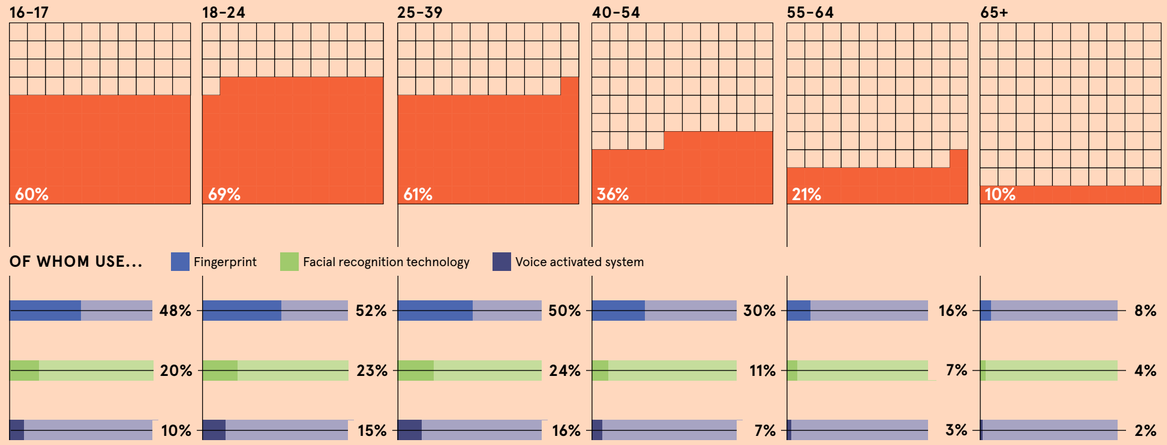


Paysafe 2019

HOW PEOPLE ARE USING BIOMETRICS TO MAKE PURCHASES

The percentage of consumers using new authentication technologies to make payments, by age group

Paysafe 2019



WHAT'S HOLDING BIOMETRICS BACK?

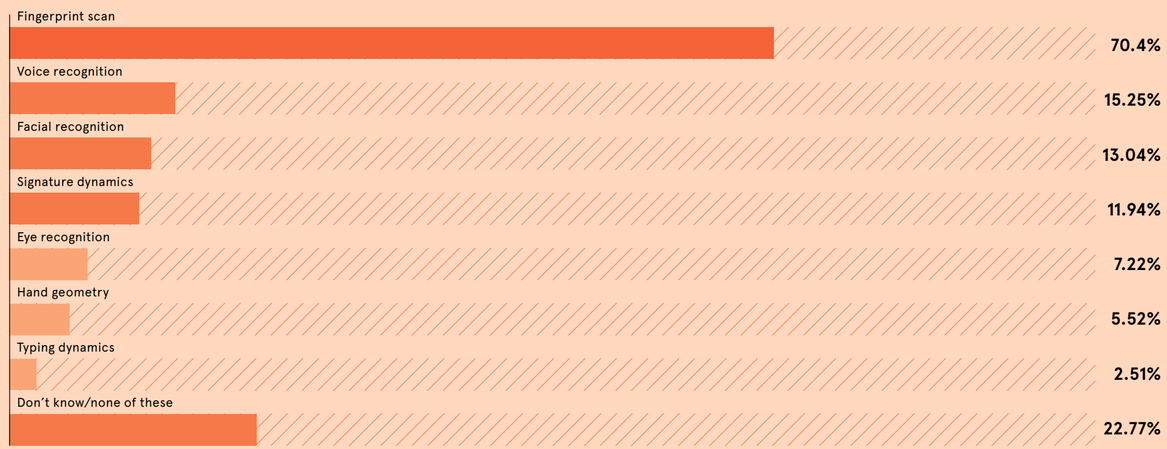
Two-thirds of US consumers have some concerns about biometric authentication

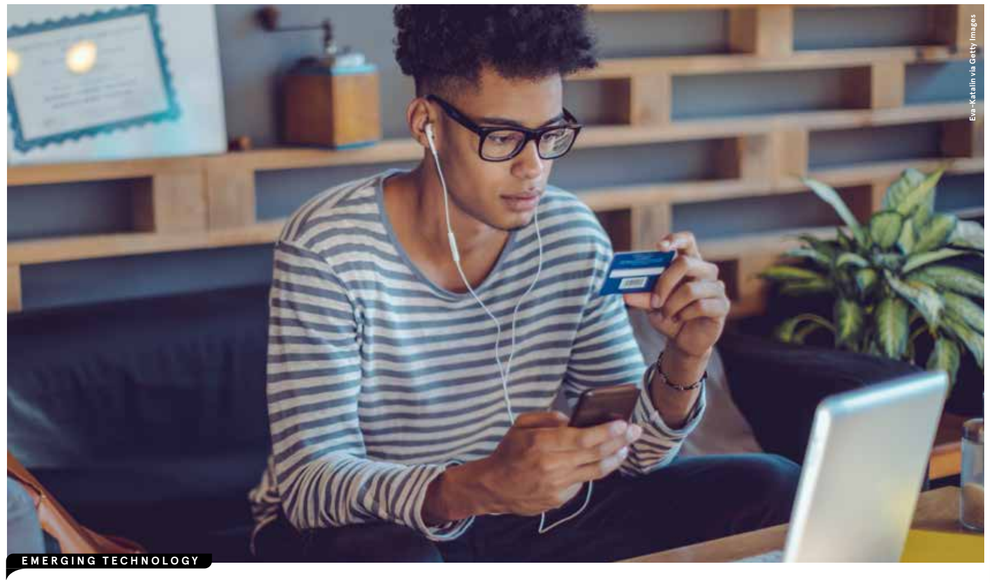
Statista 2019

WHICH BIOMETRICS ARE CONSUMERS USING?

Usage of biometric technology among US consumers

University of Texas 2018





EMERGING TECHNOLOGY

The importance of building trust in new tech

When it comes to new technologies, speed of adoption relies on user trust, making it important for companies to understand how to build that confidence

Sanjana Varghese

Since coronavirus struck, trust in the technological platforms and services that underpin essential processes has been crucial to keep the world moving.

Employees working from home need to trust they will not reveal sensitive company information through accessing servers remotely. People buying groceries for shielding family members have to make sure their sensitive information is not at risk of becoming public without their knowledge.

Before COVID-19, the digital identity sector was growing. Now the role of consumer trust in speeding up adoption of digital identification technologies is more important than ever.

Rachel Botsman, the world's first trust fellow at Oxford University's Saïd Business School and an expert on the relationship between trust and technologies, says the role of trust is vital when developing any technology, not just digital identity technologies.

"If you don't have faith or confidence in a system, then you're just not going to use that product or those services," she says. "We can define trust as a confident relationship with the unknown, so if we're accepting that presence of digital identification technologies within our lives, it will often require accepting we might not know many of the technical details about the systems used. But this is asking a lot for something that may not actually be very familiar to us."

In 2019, British Airways was fined £183 million for a data breach when more than 500,000 customers had their details harvested by hackers. But the airline didn't disclose the full number of transactions that had been affected or the amount of information which had been released. In November 2018, Uber disclosed it had been attacked by hackers in November 2016 and was handed a £400,000 fine. These events can leave what Botsman calls "trust scars".

She explains: "Concerns about privacy and security have really grown in the past few decades, but context is king here. We may have more trust in digital identification technologies around banking because we've been involved in authentication in that sector for over a decade now."

But it could be a different story when it comes to a relatively controversial or intimate field, such as the creation of a digital health identity. People can't be forced to feel comfortable with these technologies overnight; companies have to work to show consumers they're not going to let them down.

One method for companies looking to build up trust is to emphasise their product or service isn't wholly new and unfamiliar. Vanessa Viala at Thales Group says companies can build trust in new technologies by understanding that, while it can't be rushed, it can definitely be helped along by tapping into the trust that exists between consumers and the technology they already use.

Apple uses a version of this process in its product design through so-called skeuomorphism, or reducing the unknown elements of a new technology and drawing on what is familiar to engender a greater sense of trust.

Companies working in digital identity can do this too. Viala explains: "Take the mobile phone. It has quickly become the personal companion for increasingly sensitive services and, as a result, a key tool in building trust. The more people trust their mobile device for payments, ticketing and mobile banking, the better we can educate the public on why digital identification technologies are trustworthy. The key is to highlight why it's secure for the end-user, as the convenient part is often obvious."

A second method is to identify trust influencers, people who can talk about products and services in a way that inspires trust on an individual level. In practice, this can mean asking experts in the field to give your product the stamp of approval, as is often the case with new forms of social media.

A final trust-building method is to make it clear to users what they stand to gain from these technologies. "You have to address what people are frightened of and so you have to emphasise what people are giving up, but also what they're gaining," says Botsman.

"You have to address the fact that how much trust is required is going to be dependent on that person and their familiarity with these technologies. One big mistake often made in launching new technologies is assuming everyone is in the same trust state."

A new generation of digital identity technologies that are decentralised and could mean every individual holds their own verifiable credentials could also hold the key to trust in the sector.

"Many people's mental modes of how systems work are rooted in these experiences, such as logging in with emails or OpenID," says Kaliya Young, a researcher into digital identity. "But decentralised identity technologies will also change these paradigms. They will provide ways for individuals to prove information about themselves and so issue any person or entity with the ability to issue verified credentials. This kind of technology would make you the host of your own login capabilities."

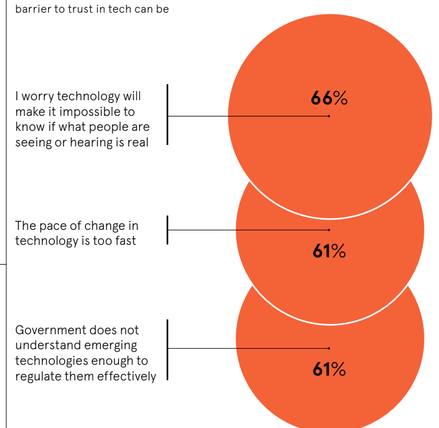
Despite steady growth in the digital identity sector, a global identification gap - where basic necessities in many countries, such as registering for a school or a job or receiving government assistance, requires individuals to prove their identity - remains. Those creating the technologies to solve this have a big job ahead and they must make building trust in their innovations a priority.

The road to trust is never straightforward, particularly in such a rapidly changing sector. "We shouldn't underestimate the power of the word identity itself," says Botsman. "Particularly when we're talking about digital identities, even the word itself is evolving."

> **One big mistake often made in launching new technologies is assuming everyone is in the same trust state**

TRUST IN TECHNOLOGY IS AT AN ALL-TIME LOW

A survey of more than 34,000 people across 28 markets shows just how high the barrier to trust in tech can be



Edelman 2020

Future of digital onboarding is super fast, orchestrated and intelligent

In the wake of the coronavirus, with lockdowns and stay-at-home orders in place, digital onboarding is often the only way consumers can be verified by businesses, institutions and governments worldwide

Use cases for biometric authentication have exploded, whether in education or COVID testing, verifying unemployment benefits or online gaming.

"In a post-pandemic world these use cases of digital verification are unlikely to go away. They are here to stay. The process is increasingly embedded in people's lives as many more of us are getting used to verifying our identity in this way. COVID-19 has not only been an acceleration event, but one that's crystalised the industry," says Labhesh Patel, chief technology officer and chief scientist at Jumio, a global leader in end-to-end identity verification and eKYC (electronic know-your-customer) solutions.

"Right now, the amount of fraud we are seeing when it comes to digital onboarding is eye opening. The pandemic has fuelled that. There are 3,500 authorised types of ID used worldwide. With so many new use cases and forms of identity to verify, you need increasing volumes of data to work out who is real, who is a fraudster, are they using a fake ID, and you need to be able to do this in real time."

Jumio has verified more than 300 million identities in over 200 countries and territories from web and mobile transactions. It has trained its artificial intelligence (AI) and machine-learning algorithms on vast datasets in a General Data Protection Regulation-compliant way in a bid to onboard customers faster and fight fraud. However, challenges remain.

"There is currently still a lot of bias in AI. Models perform well on certain datasets and ethnographic profiles, such as Caucasian identities, but not on other ethnicities, yet. This is not easy to solve unless you have a lot of representative data. It can mean certain sections of the community are not onboarded easily. There is a disparity and this is an issue we are trying to solve at speed," says Patel.

"Using human verifiers alongside data models is crucial in this process as it validates the machine-learning models. It takes a lot of time, effort and investment to clean, label and verify datasets to combat bias. For Jumio it is a top priority and we are getting there."

95%

of RFPs for document-centric identity proofing will contain clear requirements regarding minimising demographic bias by 2022

Gartner

According to Gartner, by 2022 more than 95 per cent of requests for proposals for document-centric identity proofing, which involves comparing a government-issued ID to a selfie, will need to contain clear requirements minimising demographic bias, an increase from fewer than 15 per cent today. Addressing this inherent bias in systems will be vital for the industry.

"Many people also don't realise that not all digital verification systems are created equally. The volume of data you need to work with really matters if you really want to spot fraud. The larger the referenced database the easier it is to find. Fraud only occurs in 1 to 2 per cent of all cases of digital onboarding. If you've checked a million forms of ID documents rather than a thousand, you are in a better place to know your customer and what is real or fake," says Patel.

The next frontier for digital identity proofing involves going one step further and employing additional fraud signals to increase the level of identity assurance. Instead of only relying on a government-issued ID and a selfie to onboard a customer, enterprises can combine this with address databases, geolocation information or email verifications.

"The industry is moving toward 'orchestration as a platform' where businesses can dip into other databases to verify and cross-check IDs, as well as use a toolkit of verification tools, including advanced liveness detection and face-matching technologies, as part of an automated identity-proofing scheme. It will become super-personalised based on the business customer's demands," Patel points out.

"We call it the KYX platform, moving beyond 'know your customer' to know your x, where x could be a user, patient, employee, business partner or student, but also using many more points of reference to achieve a high level of identity assurance. This is the new imperative, connecting and cross-referencing third-party data intelligently and seamlessly depending on specific use cases, risk appetite and budget."

There are several converging trends that are driving a greater demand for an orchestrated KYX platform. Over the last two years, there have been many large-scale data breaches where hundreds of millions of records, including names, emails, usernames, passwords and other personal information, have been hacked. Therefore, it's unsurprising that usernames, passwords and other personal information, including ID documents and selfies, can be purchased on the dark web for just a few pounds or dollars.

> **Fraud only occurs in 1 to 2 per cent of all cases of digital onboarding. If you've checked a million forms of ID documents rather than a thousand, you are in a better place to know your customer and what is real or fake**

At the same time, the regulations and fines from governments for regulatory compliance have risen and the COVID crisis has seen a wholesale shift to digital onboarding. It is the perfect storm. Layering a number of verification services to combat these issues and increase the level of identity assurance is essential.

Striking the right balance between accuracy, speed and the user experience is also important. Enterprises can lose customers if the onboarding process takes too long, is not seamless or involves too much effort.

"Speed is vital. We are focusing now on delivering much faster digital verification that is accurate and does not compromise the checks we need to do when it comes to fraud. Already we can get below 10 seconds to verify an ID and a selfie, but we can go further. Our mission is to automate the onboarding process, simplify KYC and anti-money-laundering compliance, and eliminate the friction and resulting abandonment; that's the holy grail. We will see many more use cases and adoption," says Patel. "This is the future."

For more please go to www.jumio.com

jumio

CYBERSECURITY

Identifying identity fraud threats

Online fraud has accelerated during the coronavirus pandemic, meaning organisations must be more vigilant in the face of the seemingly ever-increasing threat and its impact on business

Davey Winder

The coronavirus pandemic has had a big impact on many areas of our lives, not least our relationship with the office. Organisations have had their hands forced when it comes to accelerating digital transformation, while digitally identifying and onboarding both customers and employees has pulled focus on the digital identity sector.

It's good news for digital ID specialists, but the flipside is it's also a huge opportunity for cybercriminals engaging in identity fraud.

According to GBG, a company that claims the world's largest identity and fraud data ecosystem, identity fraud has hit a tipping point thanks to COVID-19: one in five consumers' identities have been stolen and one in three are now more worried about fraud.

GBG research also worryingly reveals that more than a quarter (28 per cent) of businesses admit to high levels of fraud being accepted by the organisation, with half (51 per cent) of those in financial services seeing fraud attempts rise.

This imbalance between criminal opportunity and organisational apathy must be addressed as newer threats combine with old and impact both businesses and consumers alike. They're threats that many businesses are simply unprepared for.

To tip the balance back in the direction of the digital defenders, we must understand what the threats are and how investment in digital identity technology can reduce risk exposure.

Frankenstein fraud

Synthetic ID, or Frankenstein, fraud combines genuine and falsified information to create a new identity. According to Keith Price, former US Department of Defense director of security operations and current cybersecurity director at Littlefish, it is "one of the fastest-growing methods of financial crime".

In July 2020, two men were arrested in connection with fraudulent applications for pandemic "bounce back" loans, totalling £550,000, using such identities. GBG's general manager Gus Tomlinson is concerned this type of fraud could be further complicated by the September 2020 database breach at Nitro PDF. Along with credit data breaches, he says, fraudsters will be able to "present corroboratory evidence of previous financial activity that could be deemed as valid proof".

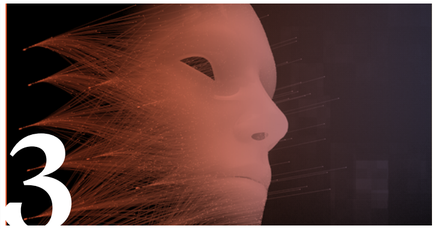
Price sees the solution sitting with businesses being "able to pivot security and fraud detection capabilities", which is where behavioural biometrics and pattern recognition come to the rescue. When 400 synthetic accounts were discovered by a European bank client, banking fraud prevention specialists buguroo deployed such a system to look under the covers. This discovered "all these accounts were linked by the fact that they were accessed by the same people, via the same device and same networks", says Buguroo vice president Tim Ayling.

Account takeover

Why go to the effort of creating a new identity when you can hijack a real one? That's the premise of account takeover, as employed in the Twitter hack of July 2020. Focusing a spear-phishing attack on a small number of employees, criminals gained access to credentials and visibility of internal processes that ultimately helped take control of high-profile accounts, including now US President Joe Biden and American celebrity rapper Kanye West. "Fake tweets were sent," Greg Chapman, chief technology officer at CM Security, explains, "which caught out respondents who engaged, and the attackers moved to steal cryptocurrency."

Matthew Gracey-McMinn, head of threat research at Netacea, warns that commonly used passwords can also be fed against known email logins using bots. "We have recently seen a streaming service hit by an attacker who tried 300,000 unique username and password combinations during a five-hour attack," he says. The 0.005 per cent success rate, with 1,500 correct guesses, is a big win. Or would have been, had the attack not been detected and blocked.

Such bot management is the best way for businesses to detect and stop these threats. Gracey-McMinn recommends using a password manager to enable unique passwords for every site and backing this up with a second authentication factor.



Deepfakes

Deepfake technology manipulates video and audio so convincingly that it presents what appears to be a real person. "The criminal underworld is not far off from making deepfake attacks look and sound truly authentic," warns Ben King, chief security officer, Europe, Middle East and Africa, at Okta. "We must anticipate a surge of attacks as criminals learn to more successfully imitate speech mannerisms using artificial intelligence (AI) layered on top of numerous voice samples from the target."

Because video and voice are more persuasive than an email or text message, deepfakes can "falsely trigger a person into an action, such as handing over data or transferring funds", according to Daniel Cohen, chief product officer for anti-fraud at RSA. Indeed, in 2019, it has been reported that the chief executive of a UK-based energy company was tricked by deepfake audio of his German parent company boss to transfer almost £200,000 in a sophisticated fraud.

While AI-based tools can help to mitigate the risk, user caution is the most effective counter weapon, says Paolo Passeri, cyberintelligence principal at Netskope. "My advice is to always double check every request," he continues. "Call the person to whom the money must be sent to verify the request is legitimate for the strongest authentication possible."

SIM swapping

In a smartphone-centric world, SIM swapping is also becoming more of a problem. Using a variety of open-source intelligence methods, trawling social media postings or corporate site profiles for example, fraudsters seek to get enough information to convince your mobile phone network provider you are the owner of the account. They then request a SIM swap to seize control of the phone number. This gives them visibility of two-factor codes sent via SMS and from there control of the accounts they protect.

Kaspersky principal security researcher David Emm points out that Action Fraud found a 400 per cent increase in reports of SIM-swap fraud last year. One couple had £25,000 stolen by an attacker while on holiday and a Californian man reportedly lost $1 million in SIM-swap fraud. Mobile providers should alert customers by SMS if there is a SIM-swap request and follow the Brazil lead by flagging banks and disabling financial transactions for the next 48 hours, Emm adds. John Gilbert, general manager UK and Ireland at Yubico, advises account takeover attempts can be thwarted with "stronger two-factor authentication, boosting login security beyond just SMS text messages".

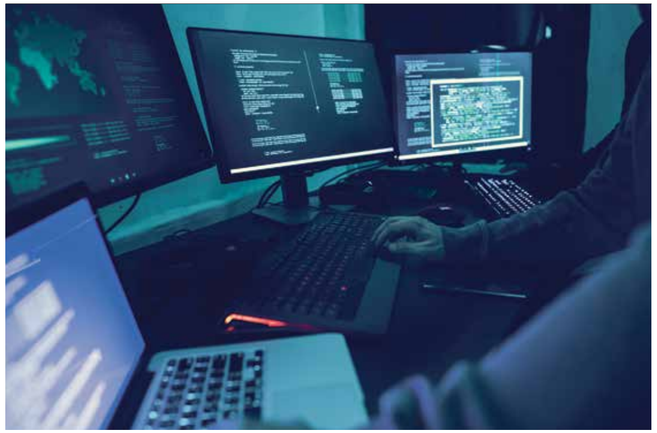
Replay attacks

A replay attack happens when an attacker sits in the middle of a supposedly secure communication, intercepting the traffic and then resending the communication later, often to conduct financial fraud. An attacker could fool the victim into completing a transaction to them rather than the originator, for example.

"In such a case the attacker is able to capture even an encrypted message and send again with the extra payload, with the original encryption still in place," says Steven Jupp, chief executive at High Impact Office. A protocol designed to protect devices against such an attack, the replay protected memory block was recently found to have a vulnerability that could allow it to be bypassed. Although there are few readily available mitigation technologies on the market, Jupp says the "consensus for solution is to utilise time-stamping and random key pairs, which are used just once in a message transaction".

He also suggests that incorporating unique verified packets into the messages could provide an ability to verify the message came from the correct device, which wouldn't be possible by resending. Blockchain could be of help, but Jupp warns of "inherent risks with utilised public blockchains, plus delay and costs when sending large data sizes".

Commercial feature



Getting forensic to turn away the hackers

The SolarWinds attack is the latest in a long line of hacks targeting identity infrastructure. To prevent being the next victim, organisations need to know which keys have been issued

The data breach on US software company SolarWinds was another reminder that core enterprise authentication is the pivotal security challenge in modern IT networks.

Sophisticated hackers lay the groundwork for crippling attacks by first establishing persistence within trusted networks. Their most potent weapons are account takeovers and hacks of critical identity infrastructure like Active Directory, Microsoft's identity directory service, and Kerberos, the network authentication protocol.

Attacks on Active Directory Federated Services (ADFS) and Security Assertions Markup Language (SAML) often then follow.

This was exactly the case for SolarWinds, whose customers were the ultimate targets, and the consequences were not only grave but embarrassing and still unfolding. Serious data breaches were felt widely across US government departments, as well as numerous large tech companies, after the attack went undetected for many months.

Yet given that lateral movement techniques during key stages of the attack were similar to the 2014 hack of the US Office of Personnel Management, much of the impact could have been prevented with better detections for Kerberos, ADFS and SAML-based identity attacks.

"We have to take a real hard look as a society and say, if we're going to build treasure troves of data, we need to know we're keeping track of the keys issued to access it," says Jason Crabtree, co-founder and chief executive of risk technology firm QOMPLX.

"If you just outsource everything with identity, your entire security model is premised on somebody else not screwing up. Organisations must actively decide how to get control and visibility of authentication because if they can't track exactly what they're doing in their own identity environment, they won't be successful in their security programmes.

"Regardless of who you use for identity, and most enterprises find they need a hybrid identity path, you must be sure they're not just looking at log data. To get the full history of who logged on to what and when, and have some ability to audit what happened on a network, they need dedicated controls looking directly at Kerberos, ADFS and SAML exchanges.

"Too many organisations don't have any post-forensic ability to reconstruct the details of what happened during major breach events because they didn't collect the necessary data in the first place. That ought to concern both companies and regulators."

QOMPLX, which validates billions of Kerberos transactions globally each day, was publishing warnings back in 2018 and 2019 about ADFS-based attacks linking on-premise Active Directory compromise via Kerberos ticket forgeries to ultimately malicious SAML token issuance.

Its Q:CYBER solution is the most comprehensive and accurate tool for detecting advanced lateral movement techniques that exploit Active Directory and enterprise authentication protocols like Kerberos, SAML and ADFS.

By fusing unique authentication data with multiple log sources and security data feeds from endpoint, perimeter and cloud vendors, QOMPLX gets to the ground truth in security. It has spent the past six years developing powerful streaming analytics, graph capabilities and related services to harden enterprise authentication, secure Active Directory and bring together the data sources inside and outside corporate networks.

"We initially specialised on attacks that forge or create fake authentication tickets or tokens, developing and patenting technology that allows us to collect specialised data you just can't get out of logs," says Crabtree. "You need live instrumentation, and to reconstruct and keep a full ledger that provides a chain of custody, knowing this key or token was issued to this person who presented it to this service which took this action.

"Why? Because lateral movement via authentication protocol abuse didn't just underpin the SolarWinds attack; it's part of virtually every major breach or ransomware event. It's completely detectable with our solutions, already deployed in some of the world's largest companies. You can't prevent every attack, but by responding faster you can prevent the perpetual breach escalation when you only find out about it ten months later."

For more information please visit QOMPLX.com

QOMPLX:

CUSTOMER EXPERIENCE

How 'positive friction' can create better experiences

Businesses have strived to eradicate friction from their customer experience, but have they gone too far?

Duncan Jefferies

When it comes to customer experience, friction is as frowned upon as confusing web design and poorly trained staff. It annoys consumers and can cost sales. At least that's been the prevailing view of businesses in recent years. But what if they're wrong? What if some friction is (whisper it) a good thing?

"Businesses have the current mindset that the pinnacle of great customer experience is a frictionless transaction," says Amir Nooriala, chief commercial officer at Callsign, which provides identity authorisation and authentication solutions. "Instead, customer experience is increasingly about creating a personalised journey that delights the customer."

Up until now, businesses have focused on using technology to minimise friction and create seamless customer journeys. "However, it's time to change that mentality because it's not always about eliminating the friction out of identification altogether, it's about putting it in the right place and at the right level for each individual," says Nooriala.

It could be argued that banks and merchants have only been trying to give customers what they want: smooth, hassle-free experiences that don't require them to re-enter a password or retrieve an SMS code from their phone. But it's increasingly hard for businesses to strike the right balance between eliminating fraud and managing friction, says Gus Tomlinson, general manager at GBG, an identity management and fraud prevention company.

"Why? Because the competition is huge and consumer attention is short lived. Businesses know they need to deliver a seamless customer experience to attract and retain customers, but as the world speeds up businesses should be careful not to go too far," she cautions.

In ecommerce, cutting five seconds from the average transaction can reduce cart abandonment and ensure the transaction is completed, says Nooriala. But if account information is compromised, the consumer will have to work with their bank to address the problem, wait for a new card to be issued and manage a whole new authentication process, which is the very opposite of a friction-free experience.

Taking a personal approach

Businesses that are prioritising frictionless experiences above all else also risk alienating some customers, particularly when it comes to onboarding processes or large financial transactions.

"A quick process or transaction isn't necessarily one that's trusted by the customer," says Tomlinson. Research carried out by GBG in December found less than a sixth (15 per cent) of customers think it's important for account opening processes to be quick and less than a quarter (23 per cent) think simplicity is important. More than half (52 per cent) believe security should be the main priority.

However, Tomlinson points out there isn't a one-size-fits-all approach. The research also found younger customers, aged between 18 and 34, were less interested in the sign-up process being secure and more concerned about speed and ease of use.

Likewise, some consumers will prefer biometric login processes and others the more traditional password method. Preferences can also vary across companies, with customers welcoming less friction from well-known or regularly used companies and more from new or unknown ones.

> **A quick process or transaction isn't necessarily one that's trusted by the customer**

Some organisations adopt the concept of a "soft login" from consumers' known devices, says James Squires, lead consultant of tech strategy at agency Wunderman Thompson Technology. This might mean, for example, that initially registering or entering login credentials would enable features such as personalised content or the ability to add items to wish lists or a shopping basket without re-entering details. Login credentials would only be needed again at the point of making a purchase.

Ocado is a good example of a company that has got this right: users can choose products and arrange deliveries, and only have to submit their credentials when placing an order. Amazon goes a step further by offering their customers the option to switch on one-click purchasing, although this is only for delivery to an address that already has a payment method paired with it, Squires points out.

Harnessing positive friction

Even when friction does trigger some negative emotions in the consumer, these are often counterbalanced by the sense that the company is taking sufficient care with their personal information.

"Trying to eliminate, rather than harness, negative emotions like friction can be a mistake," says Joana de Quintanilha, principal analyst at Forrester.

For example, when Fidelity Investments examined the journey customers take to grant others permission to trade on their accounts, they found that making this process completely frictionless was not something their customers appreciated.

"They didn't mind the extra hurdles and time it took if it meant Fidelity was performing background checks and taking other security precautions to keep their accounts safe," Quintanilha explains. "A little bit of friction in that particular context actually created confidence in Fidelity and the safety of their data and accounts."

The way customers respond to friction often relates to the value of the information that could be compromised. "Customers will naturally expect and tolerate more friction for high-value targets like large monetary transfers and medical records than they would for their digital magazine subscription," says Jenn Markey, director for identity solutions at Entrust, which enables trusted identities, payments and data protection.

Friction and security aren't mutually exclusive, of course. Biometrics and secure tokens matched to a verified ID on file can reduce friction without compromising security. Smartphone scans of driving licences and passports for remote identity verification, as well as proof of "liveness" via short video recordings, also scratch the consumer itch for both secure and relatively fuss-free account-opening processes.

"New technologies that enable businesses to reduce friction provide better security than before," says Nick Caley, vice president, UK, Ireland, Middle East and Africa, at ForgeRock, an identity and access management software company. "This is because traditional usernames and passwords are huge security risks."

The World Economic Forum found four out of five data breaches are caused by weak or stolen passwords, usually because people recycle the same credentials across accounts in an effort to remember them.

Digital security education

The Investing and Saving Alliance (TISA) is spearheading development of a digital identity scheme for UK financial services that will allow consumers to set up a reusable digital identity. It aims to reduce friction for a range of different transactions, such as opening an account, that should increase conversion rates while delivering a better customer experience.

The project team has undertaken research that found consumers want both security and ease of access. "The critical issue is to explain how their personal data is going to be used and that different checks can happen in the background, such as anti-impersonation checks," says Harry Weber-Brown, digital innovation director at TISA.

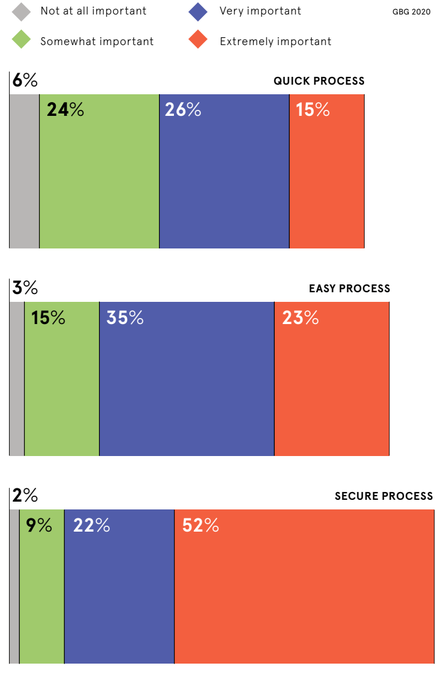
As such, the digital identity scheme is developing a consumer pledge to help users understand the safety principles and protections in place and what recourse is available should there be a breach of their data. This will be coupled with a trust mark that can only be displayed by organisations that are accredited to the scheme, which Weber-Brown says will foster trust within a low-friction customer journey.

Technology is also getting better at working out whether it's really you trying to log in or instigate a transaction, based on a series of clues that determine an overall risk score. If necessary, additional layers of security can be triggered to verify your identity, but most users will enjoy a frictionless experience.

"It will take a bit of education," says Steven Rees-Pullman, senior vice president, international, at Auth0, an identity management platform for app builders and developers. "But what's exciting is adaptive innovations represent a turning point where technology will do more of the work for us with the same, and very often better, security."

CONVENIENCE VERSUS SECURITY

UK consumer perceptions of the importance of the following when opening a new account



Commercial feature

Beyond lockdown: Kick-starting economic recovery and addressing social exclusion

Digital identity can boost economic recovery and tackle social challenges

An assured digital identity can help bridge more than the digital divide, says **Martin Wilson**, chief executive of Digital Identity Net

We are all very aware that the past 12 months have transformed almost every aspect of our lives, forcing all of us to adapt in ways previously barely imaginable. From kitchen-table offices and schools, to digital socialising and the increased dominance of online shopping, our lives have changed significantly. However, while we have all faced lockdown challenges, their impact has been felt very unevenly across society.

The first lockdown resulted in the biggest decline in the UK economy on record, contracting by 19 per cent in the second quarter. Lockdowns two and three have dealt further body blows to the economy, forcing many thousands of businesses to permanently close their doors and the UK's unemployment rate to rise above 5 per cent for the first time in over four years.

Existing social inequalities have been exacerbated by the digital exclusion of many vulnerable sections of society. This exclusion is much more than simply a lack of reliable online access, though this has certainly resulted in lost education opportunities for many less-privileged children.

The digital shift of so many aspects of our lives has created new challenges for individuals to prove their identity online, impacting access to finance, health and other essential services. It has also increased opportunities for criminals to prey on the vulnerable. From a business perspective, complex online customer sign-up processes are driving abandonment rates ever higher as consumers simply give up trying to complete frustrating form-filling tasks.

While an assured digital identity solution can help tackle the social menace of fraud, it can also address several aspects of social exclusion, which the pandemic has accentuated. At the same time it can provide a much-needed kick-start to economic recovery.

Fraudsters actively target vulnerable individuals through impersonation and identity theft. A Policy Exchange study estimated a £4.6-billion increase in online fraud since the start of the pandemic.

One particularly cruel form of such cybercrime is so-called romance fraud, where criminals create a fake profile on a dating website to lure users into handing over money. Charity Action Fraud suggests this type of scam has increased by 15 per cent over the past year, with more than £63 million stolen in 2020. If dating platforms introduced an assured digital identity, opportunities for this form of fraud would be significantly diminished.

Another alarming growth area under the pandemic is gambling misuse. Perhaps unsurprisingly, use of online gambling apps has increased during the successive lockdowns and along with it access by underage as well as addictive gamblers. Enabling the gaming sector to validate the true age and identity of an individual is a powerful tool in tackling the social harms that derive from gambling misuse, such as addiction and mental health problems.

The economic recovery, which we all so desperately wish for, is an example of where an assured digital identity solution can deliver wide societal benefits. A study by McKinsey details how an assured digital identity solution could generate upwards of 3 per cent GDP growth in the UK over the next decade. Likely benefits in 2021 and beyond being significantly higher, given the economic contraction of the past year.

Such an assured digital identity solution is not some long-term technology pipe dream; it is here and accessible now. OneID by Digital Identity Net is the independent digital identity platform about to pilot with some of the UK's leading banks and businesses. Using the UK's open banking services, individuals can leverage their existing assured personal identity, held in trust by their bank, to simplify and secure their online lives.

For businesses, and public sector agencies, introducing such a frictionless customer sign-up service gives them the assurance that the person they are dealing with is verifiable through the identity details held on their behalf at their own bank.

The infrastructure and the solution is in place now. The social need is tangible. The economic benefit is significant. Together we can make a major contribution to tackling cybercriminals, healing a growing digital divide, addressing social exclusion and giving a kick-start to economic recovery in 2021 and beyond.

If your organisation would like to join the pilot or for more information please visit digiidnet.co.uk

digital identity net

GDPR

Getting data protection right: three key things to know

If data protection goes wrong it can be extremely damaging, so companies should keep up with the latest developments and best practice

Francesca Cassidy

Richard Drury via Getty Images

When the General Data Protection Regulation (GDPR) was implemented in 2018, it marked the most comprehensive piece of legislation on data security ever created. Yet, nearly three years on, too many companies are still getting it wrong.

According to research by law firm DLA Piper, UK companies have suffered more than 30,000 personal data breaches since May 2018. Last year, EasyJet was hit by a hack in which nine million of its customers had their details stolen, resulting in a total potential liability for the airline of £18 billion.

Such data breaches can cost businesses both directly, in fines and liability, and indirectly by eroding trust, which in turn can hit revenues and profit, with the impact often taking years to reverse. This means any company that needs to solicit, manage and store customer data cannot afford to ignore best practice.

However, advice around data and digital identity can be complex and confusing. Here are three key things to know when it comes to keeping customer data, and a company's reputation, safe.

1 GPG45: Verifying someone's identity

Whether a company is signing up a new customer or onboarding an employee, verifying their identity is a crucial first step. If someone is not who they say they are, they might be given access to information, benefits and services to which they are not entitled, and greatly increase the risk of fraud.

The UK government's Good Practice Guide 45 (GPG45) is designed to save organisations from this, offering a five-part process for checking identity. Housed on the government website, it is designed to make the identity verification process simple and consistent for all UK businesses, leaving fewer vulnerable to scamming.

The process begins by gaining evidence of "claimed identity", or who the person says they are, and ends with checking the identity is not only a real one but belongs to the person claiming it. Through each stage, businesses are given suggestions of the best ways to test claimed identities, what counts as an authoritative source of verification and scores to give each phase based on how thoroughly the information can be checked. These scores can be used to calculate a level of confidence in that person's identity.

2 Anonymisation versus pseudonymisation: sharing data safely

There may be occasions where a company wishes to use personal data, belonging to either customers or staff, without breaking the rules, for example when presenting research to third parties about the ways in which products or services are being used.

> **Adopting privacy by design can help greatly reduce the risk of a crippling data breach**

In these instances, it may be desirable to anonymise or pseudonymise data, but it is important to understand the difference. One type of data is protected by GDPR, the other is not.

Anonymous data, according to GDPR, is "information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". This means no names, addresses, phone numbers or photos, but also no information that could identify someone when linked with other pieces of data, such as a place of work, job title or medical condition.

Properly anonymised data does not fall under GDPR, which means it can be exported internationally and kept for as long as needed. The process of anonymisation is irreversible, however, and can devalue data or render it less useful for other purposes.

Information is only fully anonymised if there are at least three individuals to whom it could refer. And context matters. Data on gender or ethnicity may not seem like a specific identifier, but if there is only one man working in a team or only two people of colour then that data could be combined with other information to identify specific individuals.

This is known as pseudonymised data, explained in GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately".

In practice, this could mean removing some identifiable data but not all, say, removing names, but keeping job titles, or replacing an identifying attribute with another, such as taking away gender and replacing it with the number two. In these cases, it would be difficult for someone new to the dataset to identify individuals, but not impossible. GDPR still applies to these datasets.

When is pseudonymisation useful? If a company wants to share data with shareholders, another company or the general public, it could make data pseudonymous by separating it from the identifiers. Whoever is sent the dataset will be processing anonymous data at their end and therefore be exempt from GDPR. The original company, however, still has the list of identifiers, so remains subject to the regulations.

3 Privacy by design: putting data protection first

The safest way to protect customer data is to build privacy and security into systems from the very beginning.

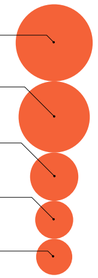
Privacy by design (PbD) is a method that can be used when building IT systems, creating strategies or policies and establishing data-sharing initiatives. The foundational principles include taking a proactive, preventative approach to privacy, rather than scrambling to deal with data breaches once they have happened and it is too late.

A PbD mindset means making systems user friendly and transparent, while not leaving the onus for privacy with the user. PbD systems should automatically protect data as a default, requiring no action on the part of the individual.

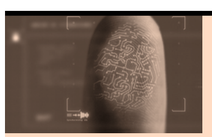
Finally, PbD means no trade-offs; privacy should never come at the expense of security. Data should be protected throughout its lifecycle, kept safe while it is under management and securely destroyed when it is no longer needed. Adopting this method and mindset should help make privacy a priority throughout the business, greatly reducing the risk of a crippling data breach.

THE WORST EUROPEAN COUNTRIES FOR DATA BREACHES

Total number of personal data breaches notified per jurisdiction between May 2018 and January 2021



DLA Piper 2021



There are seven foundational principles designed to put data privacy above all else:

1. Proactive and preventative
Rather than scrambling to deal with a data breach once it has occurred, approaching projects with a privacy-by-design (PbD) mindset means anticipating what problems will arise before they happen. Instead of spending time developing remedies for privacy-invasive events, it aims to prevent them from happening in the first place.

2. Privacy is the default
Rather than leaving privacy in the hands of the individual, PbD means ensuring personal data is automatically protected. If the individual does nothing at all, their privacy is still ensured and their data protected; it is built into any IT system or business practice as a default.

3. Privacy is embedded into design
Rather than being bolted on, or an afterthought, privacy is a central feature of the design and architecture of systems.

4. No trade-offs
Privacy does not come at the expense of functionality. Greater security does not mean less privacy. PbD believes it is both possible and desirable to have both.

5 Security through the full life cycle
Strong security is essential to privacy and it covers the data's full journey, from start to finish. This principle ensures data is securely retained, kept safe while it is under management and is securely destroyed when it is no longer needed.

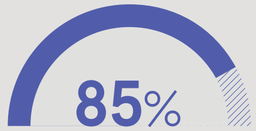
6. Keep it open
Visibility and transparency are key. A core tenet of PbD is stakeholders have full oversight of how a project is working. This means assuring everyone involved that whatever business practice or piece of technology is being used, it is being used as it was agreed to be and subject to independent verification.

7. Keep it user centric
Nothing is more important in a PbD project than respect for user privacy. Every architect and operator should keep the interests of the individual in mind at all times, making systems user friendly.

CONSUMER SENTIMENT TOWARDS THE ACCOUNT CREATION PROCESS ACROSS INDUSTRIES

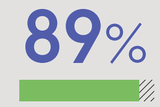
Consumer sentiment towards security checks and personal information required to open an account

Online marketplaces
85% of consumers were comfortable with providing identity data when opening an online account as opposed to only 54% who were comfortable with using biometrics as identity markers

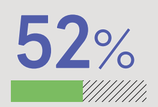


When a financial services firm uses real-time identity verification as part of their account creation process, more than 80% are less likely to abandon, 84% will have greater trust in the brand and 71% are more likely to share more personal data

Retail
90% of online shoppers cite security as a very important part of an optimal account creation experience, far ahead of flexibility (59%) and seamlessness (59%)

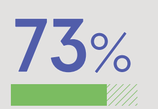


of customers think that security contributes to a great account creation experience



of consumers aged 35 under favoured speed over security in online account creation as opposed to 33% of consumers aged 35 and up

Almost 90% of online shoppers say they are concerned about identity theft when using retail sites and feel safer when sites ask to verify their identity



of customers claim that they are increasingly intolerant of poor experiences when opening new online accounts

Trulioo Consumer Account Opening Report 2020

Layered approach to assessing identity risk brings trust to the digital economy

Organisations struggling to find the balance between security, compliance and a positive customer experience online can adopt a layered, risk-based approach to digital identity

Rapid growth in online activity and the global nature of the digital landscape has amplified opportunities for sophisticated fraudsters to circumvent regulatory and compliance requirements through technology.

Synthetic identity fraud, whereby a real person's data is combined with fake information, is particularly on the rise, with Experian data showing it now accounts for 80 per cent of credit card fraud losses. The coronavirus pandemic has added extra impetus both to online activity and digital fraud.

Organisations have responded by ramping up digital identity and authentication processes, but every action has a reaction. Consumers expect a seamless, speedy user journey online without compromising security and a sub-par experience can actively deter them. A recent survey revealed two thirds of European consumers abandoned digital banking applications because they were too cumbersome.

The initial stage of an online customer journey, opening an account, is especially important in building trust and loyalty. Cumbersome onboarding can prompt frustrated customers to switch to an alternative service, hitting the bottom line, yet most UK and US consumers are unimpressed by online account creation processes.

In a study by Trulioo, fewer than half said they are satisfied with what they've experienced with marketplaces, retailers and financial services providers, despite three in four believing such processes can be a real deal-breaker for their future relationship with a brand.

Spanning different markets, industries and jurisdictions, identity verification in the global digital economy is complex. Every interaction presents a unique scenario that poses different levels of risk.

To master the balance between mitigating these risks and offering a positive customer journey, with just the right amount of friction, a layered, risk-based approach is required. Supported by global data intelligence, organisations can ensure legitimate users face no unnecessary disruption, while those deemed as high risk or suspicious are escalated for enhanced due diligence, keeping bad actors out.

"A layered, risk-based approach to compliance and anti-money laundering (AML) requirements combines a multitude of verification services that increase acceptance rates for legitimate customers and susses out malicious actors or perpetrators of fraud," says Zac Cohen, chief operating officer at Trulioo, a leading global identity and business verification provider specialising in AML and know-your-customer (KYC) compliance.

"Tapping into diverse data sources enables organisations to have complete flexibility in their AML and KYC checks dependent on the type of business or service and at each stage of the customer journey.

"By taking into account the unique attributes of their business, jurisdictions operated in and where their customers are located, organisations can tailor the onboarding experience. This means carefully considering the level of risk of each of your consumers and metering out the appropriate level of due diligence or friction. A wealth of valuable data is at companies' disposal and, as long as they are taking a privacy-centric approach, it can be leveraged to inform customer journey workflows and risk-based modelling."

> **With a risk-based approach, you can customise your user experience, ensure you're meeting regulatory requirements and safeguard your users from bad actors**

Through one single portal and application programming interface, or API, Trulioo's comprehensive identity solution enables websites and mobile applications to verify five billion people in more than 195 countries, without friction, providing secure access to a global network of reliable identity data sources and services.

With access to this network intelligence, as well as industry insights, best practices and Trulioo's technology and data partners, organisations can take a truly tailored approach to their compliance and fraud-prevention programmes.

"With global coverage, our approach is scalable, meaning organisations can easily expand to other jurisdictions, service customers in new regions and meet jurisdictional compliance requirements," says Cohen.

"We leverage artificial intelligence and machine-learning to parse through huge datasets of transactional and user behaviour to spot and provide alerts on suspicious activity. This trove of behavioural data can point to fraud signals and easily identify a fraudster or malicious actor before they can do any harm. Biometrics has also become an important data source and part of that layered approach.

"We view security, compliance and user experience as having a single common goal: trust online. With a risk-based approach, you can customise your user experience, ensure you're meeting regulatory requirements and safeguard your users from bad actors. While we have a team well versed in compliance and regulatory developments, we also have strong technical acumen that we are applying to develop a diverse range of innovative tools to build a robust digital identity network.

"Our expertise uniquely positions us to proactively suggest changes and improvements that maximise return on investment."

Trust and safety underpin all components of the digital economy, and are critical to building a credible community of users who feel comfortable transacting or interacting with others. Rampant fraud deteriorates the sense of trust and safety needed for every type of organisation to function successfully to acquire and retain their users and customers, jeopardising the integrity of the digital economy.

Trulioo is committed to recreating the trust of a village in the digital economy, ensuring no one is left behind.

"At the core of our mission is financial inclusion," says Cohen. "Much of the world does not have access to traditional identity documents or traditionally reliable sources of record, effectively shutting them out from accessing online commerce, financial services and other resources in an increasingly digital-first world.

"Alarmingly, there's also a good portion of individuals who are underbanked and excluded from opportunities for economic growth. By enabling the underbanked to safely access financial services via a mobile app, for example, we open up the opportunity for more individuals to have more freedom and control over their financial lives.

"What's more, we can rely on alternative but reliable data sources like mobile network data to verify those without conventional credit histories. This is why digital identities are so important. Of course, this means more innovative vigilance is required to mitigate risk and keep bad actors out. As proponents of financial inclusion, we're continuing to build a robust digital identity network that takes into account reliable data sources and tools to verify individuals around the world."

For more insights and data on identity verification and more, visit trulioo.com/resources

Trulioo

PERSONALISATION

Building a 'single customer view'

Investing time, resources and money to create personalised and valuable customer experiences can reap big rewards, but there are challenges in aligning data for a business-wide strategy

THINKA Via Shutterstock

Oliver Pickup

Organisations that invest heavily to build a data-driven "single customer view", enabling personalised experiences, are likely to reap huge rewards. And I can vouch for that.

At the risk of offending family and friends, by far the greatest highlight of a recent birthday was receiving a personalised celebratory email from the captain of the football club I have supported since I could kick a ball.

While it was a surprise to see his grinning portrait and accompanying message landing in my inbox, it triggered a giddy response. The feeling of being unique and valued overpowered any rational scepticism that my Premier League team's superstar skipper had taken the time to congratulate my age milestone.

This nifty, cost-effective note, made possible because the club somehow knew my birth date, emboldened my trust and loyalty. I duly spent hundreds of pounds in the online shop on kits, mugs and hats, and marked with a flag the email, which I often click on when needing either a mood lift or guidance.

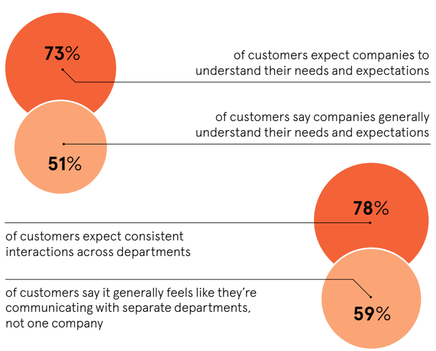
Businesses will score if they use real-time data to communicate with customers at appropriate times, and it comes across as sincere and authentic, says Adam Spearing, chief technology officer for Europe, Middle East and Africa at Salesforce. "Brands can build trust through meaningful interactions with their customers, anticipating their needs and delighting them," he says.

"Having a 360-degree customer view is crucial for enabling brands to have more personal and contextually aware interactions with customers. The more valuable an interaction is for a customer, the more inclined they will be to continue to trust a brand to use their data appropriately."

Spearing warns there is "a fine line", though: "Only if brands use the data respectfully will they gain that trust." Herein lies the main challenge with building a single customer view.

EXPECTATION VERSUS REALITY Salesforce 2020

What UK consumers expect from companies and what they get in reality too often don't align



Slow and steady wins trust

There are myriad benefits to investing in digital identity specifically to build a single customer view by unifying all relevant data into a centralised profile. Done well, aside from improving all-important customer trust and loyalty, it can guide marketing, boost customer service, better model consumer habits and, therefore, generate more accurate predictions and increase revenue.

Yet there are many pitfalls to dodge to obtain this view. For instance, brands need to connect all historical data with real-time behavioural data, which means digital identities should grow organically over time.

"Achieving a single customer view remains a huge challenge for many businesses due to the multiple touchpoints the average customer faces when dealing with an organisation and the rapid rate at which data is generated," says Gavin Laugenie, head of strategy and insight at dotdigital, an omnichannel marketing automation platform.

He points to a recent Experian study that found 92 per cent of companies do not have access to a single customer view. Laugenie says this "staggering" figure is mostly because the many touchpoints result in fragmented and siloed data. "The key to getting around this is by adopting technology that not only allows you to communicate with all of your data touchpoints, but pool the data and enable you to use it quickly and easily," he says.

A single customer view will provide the foundation from which an organisation can "easily read the data and plot the right messages to send individuals as they navigate their unique journeys with you", says Laugenie. Once armed with the data, it is crucial not to bombard customers, though.

"It's a continuous process and that mutual sharing will generate trust, which is essential, especially for older online shoppers," he adds. "Slow and steady will win the race."

The rising appetite for personalisation

Benoit Soucaret, group creative director at LiveArea, a global customer experience agency, concurs. "Good personalisation shouldn't appear personalised at all," he says. "Instead it should appear fortuitous, delivering value to a consumer at the right time, in the right place, in the right way.

"It is less about selling consumers products and more about complementing their life experiences. At no point can it appear disconcerting, intrusive or annoying."

There appears to be a rising appetite for personalisation, according to research published by the Data & Marketing Association (DMA). Some 39 per cent of consumers are "personalisation fans", a group whose members prefer offers to reflect their interests instead of being surprising. A further 33 per cent appreciate both personalised offers and those that are more random. Only 28 per cent do not favour personalisation.

"This strong desire for personalisation is encouraging for brands wanting to strengthen their relationship with existing customers," says Tim Bond, head of insight at the DMA. But he identifies something else brands seeking to build a single customer view must be aware of: poor quality or misused data.

Consider how, in January 2020, Aviva addressed its entire email base as "Michael", proving that mistakes can creep in, even with basic data. "The assumptions, errors and insults will be amplified with each step more personal," says Tom Kennedy, M&C Saatchi's senior art director.

Bond agrees: "For a centralised profile to have meaningful value, businesses must have a system in place that can analyse data on previous interactions and combine it with insights from real-time user journeys. Only then can businesses truly understand a customer's preferences and values.

"Having the right data, consent and preference management processes in place is imperative for businesses that want to guarantee and gain the maximum value for and from their customer data."

> **Having a 360-degree view is crucial in enabling brands to have more personal interactions with customers**

Connecting online and offline data

In particular, marketers understand the merits of a single customer view, according to another recent DMA study. Such a system enables brands to offer more personalised experiences (45 per cent of respondents recognised this as a benefit) and increased transparency (44 per cent gave this the thumbs up). "These are two key factors in fostering long-term customer loyalty and trust," says Bond.

Consumer expectations in this area are also rising. Some 78 per cent now expect consistent interactions across departments and four in five won't buy from companies they don't trust, a report from Salesforce shows.

Given the uptick in demand for customer personalisation, there is an urgent need for businesses of all sizes to evolve for the digital age. "The growing prevalence of ecommerce and multichannel customer journeys through 2020 only increased the importance of understanding your customers' digital identity," says Matthew Avery, enterprise sales manager at Infinity, a cloud-based call-tracking platform.

Avery argues that many businesses are not taking advantage of the technology now available to connect online and offline data, including telephone calls and point-of-sale systems. "If you're currently only monitoring the touchpoints where customers finally convert, you risk neglecting your understanding, and optimisation, of pivotal engagements higher up the sales funnel," he says.

However, Megan Jones, senior strategist at R/GA London, worries that some larger companies, where departments work in silos, are simply not set up to maximise the potential of a single customer view. "Legacy organisations struggle to execute these grand visions," she says. "This failure can be caused by many things, including a lack of digital talent or poor data proficiency. Ultimately, it comes down to a lack of strategy and understanding."

Clearly, for those who have their sights set on crafting a single customer view, the road to glory is fraught with challenges. To help guide the way, perhaps business leaders can make use of an inspirational personalised email from their favourite football team's captain, too.

CUSTOMER EXPERIENCE

What does the future of digital identity look like?

With digital identity heading towards mass adoption, the arms race to secure identities is stepping up a notch

Nick Easen

Jonathan Knowles via Getty Images

Like smartphones, wifi or cloud computing, digital identity is heading on the same growth trajectory towards mass adoption. Coronavirus has been a shot in the arm for the industry with vaccine passports for travel, dealing with voter fraud or online access to new services helping to fuel adoption.

Five years from now, many more of us will be using digital channels to verify our identity on a daily basis.

"We foresee over 6.2 billion digital identity apps in service by 2025. This will capitalise upon how important the concept of identity is to our everyday lives," says Nick Maynard, lead analyst at Juniper Research. Expect rapid growth in emerging markets, particularly in Africa, where mobile-first services help citizens access banks, loans, insurance and government services.

The tech toolkit needed to catalyse the future of this sector is already available. Estonia, which is a poster child for the mass adoption of digital ID, has been using decades-old systems. "Any changes will need social more than technical developments. No tech works without the right social context," says Dr Garfield Benjamin, researcher at Solent University.

Success tomorrow will depend on societal trust in the sector today. This will be the crucial currency over the next decade, weighed against fears of a surveillance society.

"People trusting in an organisation holding their digital identity data is going to be fundamental to any successful rollout in the future. That's one reason why social media platforms have struggled with similar concepts," says Adam Desmond, UK and Ireland country lead for Mitek Systems.

"To drive adoption, government and big tech need to create more everyday use cases for digital identities. One thing is for sure, if we don't act soon, we may miss the boat."

Answer may lie with government

Accessing government services is likely to be a silver bullet. Australia announced last year that digital identity will be a major focus of its AUS$800-million technology budget package. The aim is to help simplify and reduce the cost of interacting with public services. The UK government's Digital Identity Consultation closed with a commitment to further the use of digital identities.

"We're definitely seeing a growing appetite in government as we enter the new decade," says Kevin Trilli, chief product officer at Onfido. "Setting standards will also help overcome the risk of market fragmentation as digital IDs become more pervasive in society. With centralised standards, the government can establish a requirement for interoperability, while still allowing for companies to offer competitive differentiation on the quality of service provided."

> **To drive adoption, government and big tech need to create more everyday use cases for digital identities**

This is where the problem lies as many industry players fear a proliferation in digital identities, similar to countless passwords and usernames, will weigh heavily on the sector. If you aren't living in Singapore, Denmark, South Korea, Estonia or the Nordic countries where a single, often government-backed, digital ID reigns supreme, expect a proliferation of authentication systems.

"British society has adopted an almost 'neo-medieval' approach to digital identities. Individuals are using multiple overlapping identities across different jurisdictions, technologies and commerce," explains Amanda Finch, chief executive of the Chartered Institute of Information Security.

"Our social media accounts present who we are to the online world, our bank accounts allow us to access our finances, and our national insurance numbers ensure we're paid and taxed correctly. All these identities remain separate from each other and are not interchangeable."

It doesn't help that in the UK there's been a strong historical resistance to universal identity cards, even though it's ranked in the top ten by the United Nations e-government listings.

"The biggest barrier to making things happen is it takes years for government departments to even define what their requirements are. This, on top of lengthy, inefficient and bureaucratic procurement procedures, means the technology is often outdated or obsolete by the time it's in production," says Donal Greene, chief experience officer at Innovatrics. The spectre of universal credit looms large.

> **The need to prove who you are online in a trustworthy way will only increase**

In Estonia, albeit a much smaller country with a strong digitalisation strategy, they've had a physical ID card, a SIM card and an app, all tied to a singular digital identity that's powered by blockchain for a number of years now, the benefits of which are widely experienced across society.

"My ID card doesn't just serve as my driving licence and national health card, but also as a loyalty card for bookstores and gym membership," says Florian Marcus, digital transformation adviser at the e-Estonia Briefing Centre. "It's effectively everywhere. I can also view my tax declaration or log in to my bank."

Time for self-sovereign identities?

For those nations stumbling over personal freedoms and fears of centralised digital IDs, the future could lie with self-sovereign identity, whereby people own their personal data fully without external intervention.

"This is where individuals can create their own portable digital ID," says Mark Taylor, digitalisation and data partner at Osborne Clarke. "This also chimes well with wider developments in data regulation. The aim would be to raise the level of trust from individuals about how their data will be used and encourage greater data sharing."

This form of digital ID has privacy by design and citizen empowerment at its core. With this technology there are no central repositories of information that can be compromised.

"Within five years, enterprises and governments may no longer have dominion over digital identities; the power will instead have shifted to sit with individuals themselves. People will be able to set, manage, share and withdraw specific parts of their identity with organisations, based on their needs," according to Mike Adler, chief product officer for security at RSA.

The end of online anonymity

Another driver of change will be the shift away from anonymous or bogus profiles online to one where everyone must prove who they say they are, just as they have to in real life. The recent storming of the US Capitol by supporters of President Donald Trump, incited by social media chatter, has highlighted these concerns. It's easy to incite all kinds of trouble when no one knows who you are on the internet. This will change.

"Currently, there is very little accountability online. There is a lot of focus on freedom of speech, forgetting the responsibility of speech. We'll see stronger regulations in this space, making people accountable for sharing illegal or fake information," says John Erik Setsaas, vice president of identity and innovation at Signicat.

"The need to prove who you are online in a trustworthy way will only increase. Anti-money laundering directives will also become stronger, with higher consequences for organisations and individuals for non-compliance."

So, what of the future for digital identity beyond the next few years? There are already technologies that offer a new dawn for this sector. Beyond blockchain, quantum computing could completely change how almost every type of credential is stored and verified. This technology in the wrong hands could also allow hackers to crack most centralised databases. The arms race to secure identities may therefore have to step up a notch.

"Research is already underway on post-quantum cryptography, but the speed of this research and its implementation will depend on the success of quantum research and development," says Kelvin Murray, senior threat researcher at Carbonite + Webroot.

In a decade's time, the digital identity landscape could look completely different.

Serov Aleksei via Shutterstock

Learning from Estonia

Estonia is living proof that having a single electronic ID for government and some private services can work effectively with buy-in from the general public. The question is whether this is a blueprint for the future of digital identity in other countries. The Baltic state, with a love of all things digital, is small – Estonia's population is less than 1.5 million people – and internet penetration is high. But is it an outlier?

"We need to dispel this myth of Estonian exceptionalism, it doesn't help us and it doesn't help those trying to learn from us either," says Florian Marcus, digital transformation adviser at the e-Estonia Briefing Centre.

"The most significant problem is lack of political will to change. Some in government simply don't get digitalisation, others think it's a mere gimmick. Another group absolutely sees the benefits, but only want to support projects they can finish within their current term in office, so they can capitalise on it."

Most countries still have to solve the basic question: should the government be the one and only guarantor of a verified digital identity. This may give some citizens in the UK and United States the jitters; in other nations, the private sector is playing a decisive role, such as the banking sector in the Nordic countries.

"It mustn't be forgotten that it's taken Estonia decades to achieve this with its digital ID. Programmes cannot be rushed or they will end in disaster," explains Matt Aldridge, principal solutions architect at Carbonite + Webroot.

"This is not a glory option for any one leader, cabinet or party. It relies on co-operation from a succession of governments to deliver on the promise of a unified national digital identity that is fully integrated into all citizens' daily lives."

Estonia's successful digital ID is now enabling other solutions. The government in Tallinn has partnered with the World Health Organization to create a blockchain-based, coronavirus vaccination certificate.

"The secure, private solution has successfully gained the trust of Estonians, who are used to its technology and understand how it can support public safety during the current pandemic," says Amanda Finch, chief executive of the Chartered Institute of Information Security.

The Estonian government is also looking to use artificial intelligence (AI) to deliver the kind of tasks that usually require a phone call or an in-person visit to an official agency. Called #KrattAI, the AI-powered bot or virtual assistant could soon deliver public services safely and securely.

"We could also drive this further into the private sector, but that's where we will face more questions related to ethics and privacy, and rightly so," says Marcus at the e-Estonia Briefing Centre.

"Imagine you could log in to Facebook or Twitter with your real digital identity. No more spam bots, no more opinion hacking such as we've seen with Cambridge Analytica. This could drastically increase the accountability of individuals when it comes to harassment and cyberbullying.

"But also no more secrecy for whistleblowers and a greater potential for government supervision." There's a fine balance to be had.

ESTONIA LEADS THE WAY ON DIGITAL IDENTITY Enterprise Estoni, 2020

98% of Estonians have an ID card

76% use their ID card regularly

16% of voters use Mobile ID

70,000 people have applied for e-Residency

Mitek

When you know your customer, you can say *“yes”* more often.

By combining the world’s best forensic experts with the industry’s most advanced technology, only Mitek delivers banking-grade identity verification with the highest possible assurance levels that can reduce fraud and cut costs.

Discover more at MitekSystems.com