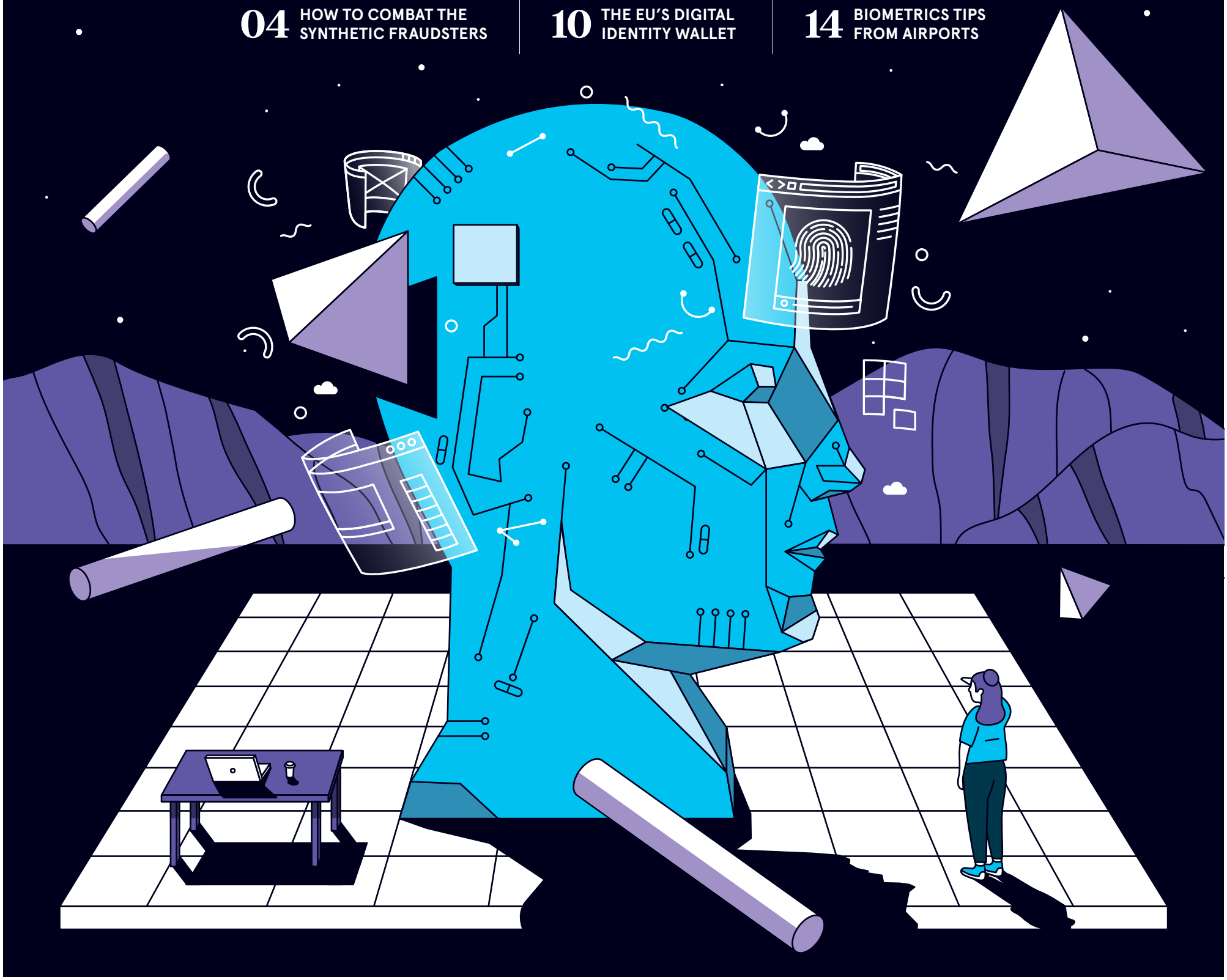
# AUTHENTICATION & DIGITAL IDENTITY





AUTHENTICATION & DIGITAL IDENTITY

Distributed in THE TIMES

Published in association with fido ALLIANCE | simpler stronger authentication



**Contributors**

**Martin Barrow**
A former health editor and business news editor at *The Times*, specialising in the NHS and social care.

**Christine Horton**
A long-term contributor to specialist IT titles who writes about technology's impact on business. She is also tech editor at B2B agency alan.

**Emma Perry**
A lab technician by day and freelance journalist by night, with a PhD in materials science from Oxford.

**Emily Seares**
An award-winning journalist specialising in fashion, retail and luxury, writing for the *Daily Mail* and *Drapers*.

**Mark Walsh**
A New York-based writer covering business, tech and media.

**Ben Edwards**
A freelance journalist who specialises in finance, business, law and technology.

**Natasha Khullar Relph**
A freelance journalist who has been writing about technology for the national press for more than 20 years.

**Tom Ritchie**
A business journalist specialising in human resources, leadership and the future of work.

**Paul Sillers**
A London-based aviation journalist and columnist covering all aspects of air travel.



Raconteur

Campaign manager
**Alfie Turnell**

Editor
**Sarah Vizard**

Deputy editor
**Francesca Cassidy**

Reports editor
**Ian Deering**

Deputy reports editor
**James Sutton**

Chief sub-editor
**Neil Cole**

Sub-editor
**Christina Ryder**

Commercial content editors
**Laura Bithell**
**Brittany Golob**

Associate commercial editor
**Phoebe Borwell**

Head of production
**Justyna O'Connell**

Design/production assistant
**Louis Nassé**

Design
**Kellie Jerrard**
**Harry Lewis-Irlam**
**Celina Lucey**
**Colm McDermott**
**Sean Wyatt-Livesley**

Illustration
**Samuele Motta**

Design director
**Tim Whitlock**

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net
Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net
The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher. © Raconteur Media

@raconteur raconteur-media @raconteur.stories

raconteur.net /authentication-2022


INCLUSION

# Keeping digital IDs secure yet accessible

Millions of people are still without a digital identity, often because of a disability or lack of access to technology. How can businesses remove barriers without dropping their authentication standards?

Martin Barrow

While most people barely give their digital identity a second thought, it's an unavoidable part of modern life. We need a digital ID to open a bank account, if we move home, start a new job or access healthcare, for instance.

For most of us, this is as simple as completing an online form as instructed, clicking on 'send' then setting about using a new phone contract or a renewed driver's licence.

But for a significant minority, obtaining and maintaining a digital ID is difficult, sometimes impossible. This means they might not have access to essential services or that their choices are severely restricted.

The reasons for this are complex. In parts of the world, access to the internet is a major problem. But even in developed nations, including the UK, many people might be unable to get this vital ID for a raft of reasons, from physical or mental disability to homelessness or immigration status. And a digital ID is not permanent, as it can be disrupted by a change of name or gender, gaps in employment or residence history. Students living at university can find it problematic if all the information on them relates to their parents' address.

But the people most likely to have difficulties with their digital ID are also those most likely to need support from the state or a local authority because they are vulnerable. So says Anna Hirschfeld, director at Public Digital, a consultancy which has worked on government programmes such as Universal Credit. "There are big challenges as more services move online. I don't think that these are insurmountable but we need to understand that you can't solve this with an app," she adds.

Identity verification is, by design, a barrier intended to ensure the right person gains access to information, services or money. But the more hurdles there are to deter hackers, the harder it becomes for people to access a system for legitimate reasons.

Freddie Quek is chief technology officer at *Times Higher Education* and leads on digital inclusion at BCS, the Chartered Institute for IT. As he sees it: "Organisations often take the view that if they are reaching 80% of their target audience, then that's good enough. But 20% of a big number is still a big number and needs to be addressed."


Jessie Casson/via Getty

To this end, the Digital Poverty Alliance is bringing together businesses and public sector organisations to share best practices and reduce the risk of digital ID exclusion.

Likewise, digital ID services start-up Yoti is just one firm tackling these problems in the private sector. It is working with companies such as Instagram and the Post Office to improve the processes they use for verification. Florian Chevoppe-Verdier, public policy associate at Yoti, says that organisations must look continuously at their processes to make them more inclusive. "As a company, we ensure that there are physical, accessible routes for people to do everything in person," he explains. "With the Post Office, for example, you can start your digital journey with a postmaster who is trained and certified to handle your personal information."

Yoti has been working hard to improve accessibility to its app-based systems and processes and has recruited an external consultancy, the non-profit Digital Accessibility Centre, to test its solutions from a user's point of view.

"When we looked at these issues, we discovered that making ourselves accessible isn't as simple as we first thought," says Chevoppe-Verdier. "As someone without a disability, it was sobering to learn how the things I take for granted can be a struggle for someone with certain disabilities.

"We had to think about everyone. This includes people with photosensitive epilepsy, cognitive disabilities, mental health issues and motor disabilities. We also needed to share this knowledge across our product and design teams and measure our progress on this journey."

Hirschfeld thinks it is critical to ensure a service design is open to change and to use alternative routes to verify identity. Organisations should also be more open to questioning the need to verify a person's identity in the first place. "If you can avoid the need to verify someone's identity, you should. Maybe you just need a secure account or perhaps to send a one-time code to users," she suggests.

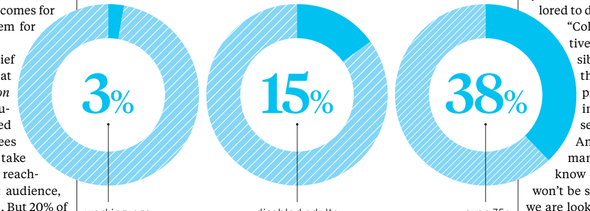
Businesses have an important role to play in improving digital accessibility. But in practice another interaction perhaps matters even more to the most vulnerable people. Many of these users rely heavily on services provided by the government which, increasingly, have digital access points.

Earlier this year, the Government Digital Service (GDS) completed a discovery exercise. It pulled together existing knowledge about the problem of identity inclusion barriers, with individuals in service teams across government sharing lessons and suggestions. This resulted in a series of recommendations about 'digital vouching'. This is a system in which a third party is invited to confirm someone's identity and security questions are tailored to different types of users.

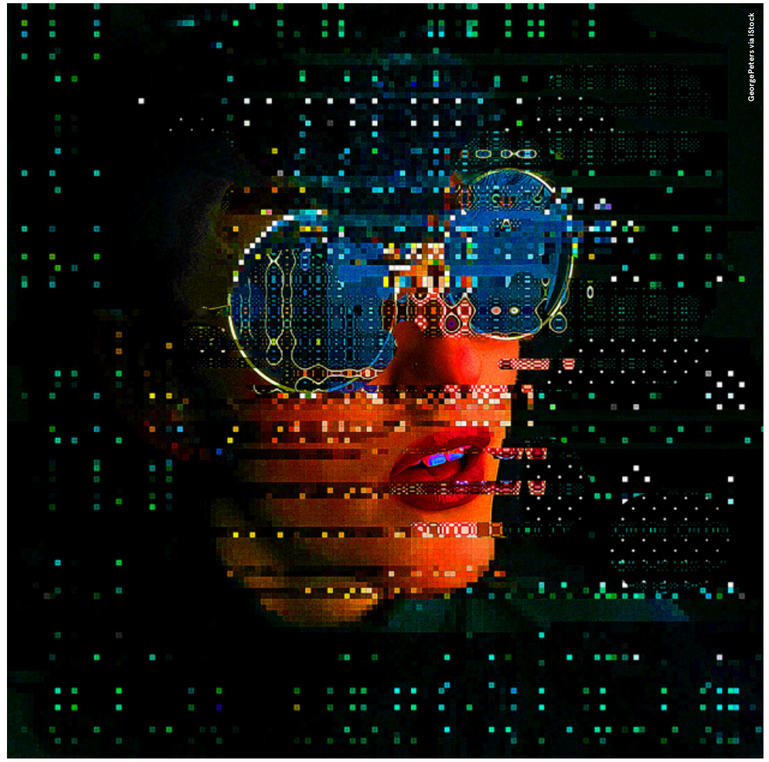
"Collectively, these initiatives will support the accessibility and inclusivity of the service. They will also provide a way for users to interact seamlessly with services," explains Ben Andrews, senior product manager at the GDS. "But we know that an online solution won't be suitable for everyone. So, we are looking at offline routes and working on effective user support channels as well."

**MANY BRITISH PEOPLE REMAIN OFFLINE**

Percentage of people who never use the internet




Office for National Statistics, 2020


GeorgePeters via iStock

CYBERCRIME

# Resisting the rise of synthetic identity fraud

Each new scam demands a new kind of defence. Now banks are using a combination of tech and human expertise to prevent losses arising from synthetic ID scams

Ben Edwards

The apartment that 41-year-old Corey Cato was renting in Atlanta had been leased under the name of Jason Brown. The problem was that Jason Brown didn't exist. Instead, it was a fake identity that Cato had stitched together from a stolen social security number and a forged driver's licence.

Cato, who has since been jailed for seven years, was part of a US fraud ring that was taking social security numbers, often belonging to children, and creating synthetic identities around them to steal almost $2m (£1.7m) from financial institutions such as credit card providers. It's a crime known as synthetic ID fraud.

McKinsey has called this the fastest-growing type of financial crime in the US. While there is no definitive data on the scale of the problem worldwide, a 2021 report from software company FiVerity estimated that annual losses related to synthetic ID fraud in the US had risen to $20bn in 2020, up from $6bn in 2016.

"The biggest thing that has promoted the growth of synthetic ID fraud is technology," explains Thomas Mangine, director of anti-money laundering and risk resilience at Canadian bank BMO. "It's easier for fraudsters to create fake documents now and merchants are selling synthetic IDs on the dark web that are being cranked out at an almost factory-like pace."

Fraudsters are obtaining the necessary personal information in different ways. One trick is to create fake job advertisements and then harvest the personal details of applicants.

"Anything on the internet can be spoofed and can look like a legitimate business or website, and people are not always savvy enough to understand whether they're interacting with a legitimate entity or a fraudulent one," explains Tamas Kadar, co-founder and CEO of SEON, a fraud-prevention company.

> **Synthetic ID fraud is not easy to tackle, but the more types of checks you implement and the more layers you add, the more accurate your system**

And fraudsters are not just impersonating individuals to access credit lines. They are also using synthetic IDs to create fake companies or even to imitate existing ones. The Covid-19 financial relief programmes gave fraudsters the opportunity to take out loans or to access grants using synthetic IDs, which were based on the partially stolen identities of company founders.

The rise in synthetic ID fraud is also proving problematic for banks that deal with cross-border entities. This is particularly the case when banks approve accounts that are based on foreign documentation.

"Increased connectivity with global markets is one of the greatest challenges for financial institutions," says Mangine. "Say you have registration documents that are written in Chinese. If you can't read Chinese, how can you recognise what looks valid or invalid? You might have a document with a lot of stamps on it and it looks like a customs document – but it might be fake."

To tackle this issue, banks are using a combination of technology and human expertise. "One of the most important things that a financial institution can have is trained investigators because nothing can replicate an active, inquisitive mind," says Mangine. "Technology such as AI and machine learning can look for the critical factors that distinguish a fraud scheme and then alert human investigators to review it."

Mangine says more tech companies are creating software to help spot the different telltale signs of fraud, though it can quickly get expensive for banks to keep pace. BMO uses a custom mix of third-party software and technology that it developed in-house to support the human investigators, he explains.

To that end, financial institutions should adopt a multi-layered approach to maximise safeguarding against synthetic ID fraud.

"There are no silver bullets to any problem. The best strategy is to use multiple solutions and stack them on top of each other," says Kadar. "ID verification is one part of the programme – which can include device fingerprinting, IP analysis, behaviour analysis and biometric authentication. The more you use, the better the security you can get."

But banks also need to strike a balance between security and being careful not to add too much friction for customers.

"When you implement too many steps in your onboarding flow, your user experience might be impacted and some customers might not finish setting up an account," he notes.

While synthetic ID fraud can be challenging for banks to spot, some clues could warrant further investigation. For instance, if there is no account activity for a significant time and then there is a sudden burst of traffic, that might indicate that the account was created using a synthetic ID, explains Kadar. Banks can monitor this by using velocity-checking tools that track the volume of activity in an account.

**US RESEARCH SHOWS THE AVERAGE SYNTHETIC ID PROFILE...**

Secures a total of
**$90k**
in stolen credit

Borrows
**$65k**
in the first six months

Has
**5**
different credit lines

Contains personally identifiable information stolen from
**3**
different people

FiVerity, 2021

Another step that banks can take to limit synthetic ID fraud is to ask customers to record themselves moving their heads and saying perfect sentences against different backgrounds during digital onboarding.

"If banks only ask for a photo against a white background, it becomes much easier for fraudsters to scale up their operation by creating deep-fake images against white walls," says Kadar. "If banks ask potential customers to move around and stand against different backgrounds instead, it limits what fraudsters can do."

Other new technologies such as analysing a customer's digital footprint or using smartphone features like Touch ID can help banks deter fraudsters because it is harder to use synthetic IDs, adds Kadar.

"It's cat and mouse. Synthetic ID fraud is not easy to tackle and it would never be possible to eliminate. But the more types of checks you implement and the more layers you add, the more accurate your system will be," he explains.

So, as fraudsters get more creative with their synthetic ID scams, it's clear that financial institutions need to be nimble when building their defences. As Mangine puts it: "Banks need to stay informed and engaged with regulators and law enforcement. And they need to talk to their own people about where the risks are in their system – then develop their solution around that."



Commercial feature

INSIGHT

# 'Sharing cybersecurity successes and failures leads to improvement'

**Andrew Shikiar**, executive director and CMO at the FIDO Alliance, explains why a culture of secrecy surrounding cybersecurity is holding back progress

If your organisation were hit by a cyber attack, would you tell anyone?

Historically, the answer would be an unequivocal no. Many believe that sharing that you were a target exposes your company's (or your personal) vulnerabilities, making you more susceptible to further attack or ridicule. But this 'security by obscurity' mindset is not only outdated, it hinders the industry's ability to harden our collective defences, most notably by eliminating our dependence on passwords and other knowledge-based credentials.

While this year saw a 5%-7% drop globally in the use of passwords for entry, it is still by far the most popular online authentication method, which is a big problem. Passwords are not only highly insecure, but they also cause major consumer headaches and are costing businesses; 59% of consumers gave up on accessing an online service and 43% abandoned a purchase when asked for a password in the past month. More than 82% of data breaches are caused by weak or stolen login credentials.

The benefits of multi-factor authentication (MFA) are widely reported but many firms have been sheepish about sharing their adoption figures.

This may be because the figures weren't great. Twitter revealed its two-factor-authentication adoption figures last summer, revealing that just 2.3% of accounts had it enabled. Of those, 80% relied on SMS-based backup, the least secure mode. Communicating this doesn't make Twitter any less secure. Instead, it sets a powerful benchmark for improvement, and gives the industry a reality check that considerable work remains to get more customers using MFA.

Other organisations to be applauded are Cloudflare and Twilio. The two cloud computing giants recently reported that they were targeted by a near-exact phishing attack. Employees were targeted with a text message from a supposed IT department, directing them to a fake website requesting a password change. Neither Twilio nor Cloudflare's monitoring systems detected the attack, and, as you'd expect, some employees were caught off-guard and shared credentials.

While Twilio fell victim to the attack (along with dozens of other companies), Cloudflare's employees were protected because they use Fast ID Online (FIDO) security keys which are tied to users. Origin binding also prevented any credentials from being shared. Since the incident, Twilio has followed Cloudflare's lead, as it shared in its updated incident report. This is a great example of how sharing successes and failures alike leads to two on the whole.

At the FIDO Alliance, we're working with the world's leading tech companies and consumer service providers to solve this challenge. Together, we've created technology that's increasingly cited as a 'gold standard' by governments, including the US's cybersecurity body, CISA, and the UK's National Cyber Security Centre.

To best defend against cyber attacks, organisations should take inspiration from the Twilio and Cloudflare story and build in security protocols that are phishing-resistant. These protocols are often implemented with USB keys or built-in biometric authentication on devices, and can be added as a critical layer of security to both an organisation's own network and information, and for customers accessing its services.

Of course, the work we do at the FIDO Alliance, creating and implementing new technology, is an important part of moving the world away from passwords and other weak forms of legacy authentication – but it isn't the most critical piece. Industry-wide commitment to creating intuitive and common user journeys, underpinned by architectural best practices, will enable the kind of cultural shift and mass adoption of this technology that will be required if we want to remove passwords from our daily lives.

Collaboration and transparency are key ingredients that raise the bar for all involved – including for hackers, who need to have a far harder time executing remote attacks. ●

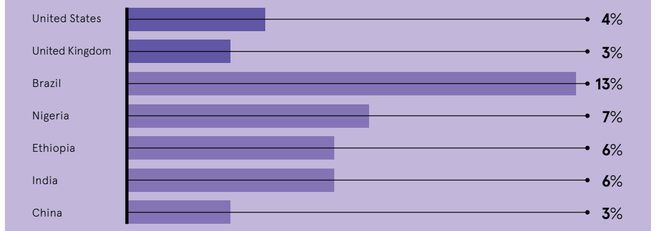
**Andrew Shikiar**
Executive director and CMO
FIDO Alliance

**HIGH LEVELS OF DIGITAL ID INTEGRATION COULD DELIVER AN INCLUSIVE GLOBAL ECONOMIC BUMP IN GDP**

McKinsey, 2019

Projected boost in economic value in % of GDP by 2030

Mature economies
Emerging economies




# Governments back a global digital ID framework. Here's why

From smart devices to biometric data, digital ID technologies are flourishing, and with them, the prospect of more inclusive economic growth

Today, a third of Estonian voters cast their votes online, using Digital ID to confirm their identity. In India, citizens can use biometric-enabled digital ID technology to verify their identity when accessing support services, such as food banks in remote areas of the country. Meanwhile, citizens in Malta can use Digital IDs to create digital signatures to secure their online transactions.

It's estimated that 3.2 billion of the world's 7.6 billion inhabitants have used some form of digital identity. However, only recently have we seen the introduction of technologies to truly protect the security and privacy of citizens.

The mass deployment of secure digital ID is becoming a reality – but globally, there are discrepancies in the rate at which countries are adopting the technology, says Steve Warne, senior director of product marketing at HID. "There have been huge projects such as Aadhaar in India, but the level of adoption is more varied around the world because of social and political issues," he explains.

One thing is certain: high-assurance verification and authentication for citizens, businesses and governments are poised to unlock substantial economic and social benefits. "The potential applications for digital ID are enormous, from tax returns to banking, passports and voting. Anywhere a citizen needs to prove their identity to the government could be made more secure and efficient with digital ID," says Warne.

> **People want to know who owns their data if they use a digital ID, and who has oversight of how that data might be used**

The concept has gained significant traction in recent years, and governments globally are on the precipice of major adoption. McKinsey estimates that some countries could see between a 3 and 13% growth in GDP by unlocking the potential of digital ID. So, why the wait?

Paper-based processes have been around for centuries, and they work. With this, the impetus for governments and businesses to optimise traditional verification procedures has been lacking. But digital transformation is booming, and extended political and economic instability means there is no time to embrace efficiency and cost-cutting like the present.

When governments integrate digital authentication seamlessly, inclusion and participation see a much-needed lift. For example, following the introduction of digital identities in Estonia, voter turnout increased as 20% of those who vote digitally would likely not vote if they were required to do so in person.

Similarly, The World Bank recently provided $100 million in funding to Rwanda to help the country implement digital transformation, including enrolling and issuing new digital ID credentials to 75% of the population. Executing trusted digital ID programmes will be critical in driving the Rwandan economy and attracting inbound investment.

The great challenge for those who deliver government services is building a business case for digital ID services and then creating programmes that are attractive, reliable and trustworthy. "The element of gaining the citizen's trust can be a big concern in some areas," says Warne. "For example, we have seen significant reluctance around digital ID for services like voting because a high number of people don't trust the technology and don't want to feel that they are being tracked."

HID is involved in around 60% of government identity projects around the world. This experience has convinced Warne and the HID team that there is an urgent need for a global framework that provides consistency and builds trust in digital ID technologies. "The industry needs to work closely with businesses, governments and regulators to create a reliable system that is transparent. People want to know who owns their data if they use a digital ID, and who has oversight of how that data might be used."

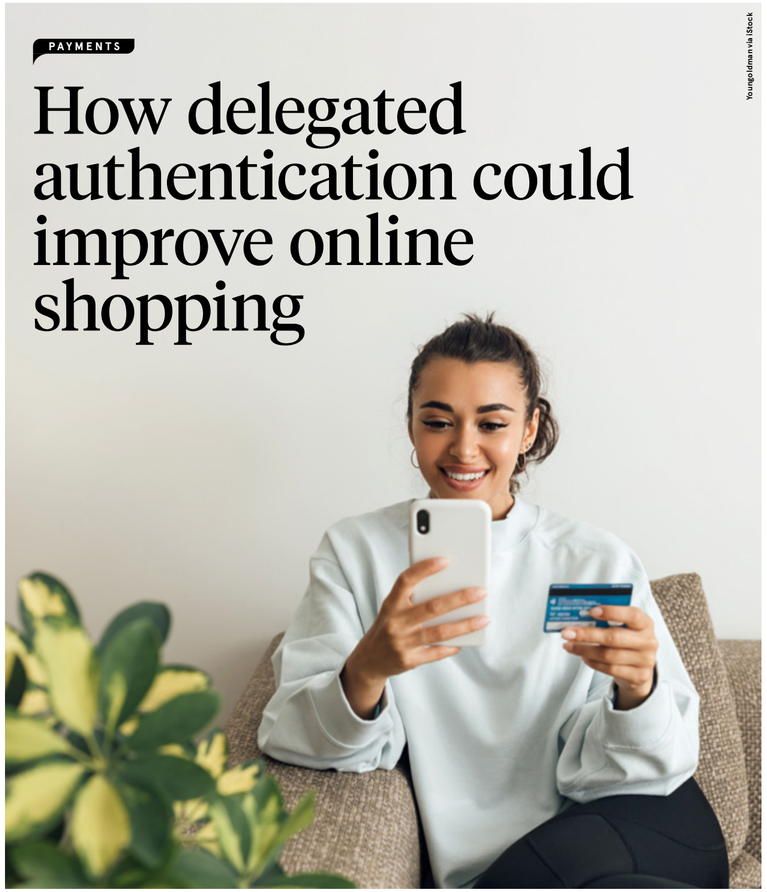
Building a business case for digital ID is more easily solved. He advises organisations considering digital ID to start building a roadmap for adoption now, focusing on adding a digital ID element to existing digital government services. "One idea is to add a digital element to existing identity document programs," he says. "If we look at a country where there isn't a strong existing infrastructure and a rural population, then a digital identity would facilitate the use of government services or even give access to banking, which could deliver rapid return on investment."

**Learn more about HID's identity management software at hid.gl/oh8**

HID

PAYMENTS

# How delegated authentication could improve online shopping



Youngoldman via iStock

Strong customer authentication has reduced the risk of fraudulent transactions but it is also stymying conversion rates. Could passing responsibility to a trusted third party offer a middle way?

**Tom Ritchie**

The introduction of strong customer authentication (SCA) for mobile payments should offer some comfort to wary online shoppers. It has, after all, made life significantly more difficult for potential fraudsters.

As part of the revised payment services directive (PSD2), brought into UK and EU law last year, customers must log into their banking app or provide a password to complete a transaction. Research by Nationwide estimates that this strengthened authentication process has prevented up to 2,000 fraudulent transactions each month. And 68% of customers say they're happy to authenticate a payment using such methods.

But SCA has also seen customer conversion rates drop. Visa estimates that as many as 11% of carts are abandoned as users cycle through apps to authorise payments.

"SCA requires merchants to think more closely about how they handle mobile payments," says Andrew Shikiar, executive director and chief marketing officer at the FIDO Alliance, a global consortium working to drive the adoption of open standards for stronger user authentication. "A lot of processes that work reasonably well on a website don't necessarily transfer that well over to the mobile experience. Juggling between devices and sending notifications for a second factor is a suboptimal user experience."

There may be a solution in delegated authentication. Here, the card issuer delegates customer authentication to a third-party payment service provider, which uses biometric identifiers such as facial recognition or a fingerprint scan. It should make payments even more secure and keep conversion rates high.

In theory, delegated authentication should make remaining compliant with the SCA regulations easier too. This is because it requires both a possession-based signifier of identity – where the transaction is completed through a known device, most likely a designated mobile phone – and a biometric signifier.

Shikiar explains that removing the use of passwords in this way has two benefits. Knowledge-based security processes, like passwords, are inherently less secure than possession-based or biometric authentication – which is much harder for malicious actors to clone and even then is "almost impossible to repeat the fraud at scale". Passwords are also easily forgotten, he says, and present a user experience problem. FIDO Alliance data shows that as many as 50% of shoppers have abandoned a transaction after forgetting their security information in the past three months, while traditional two-factor authentication, normally via SMS, is turning shoppers away.

"Knowledge-based authentication adds friction to a checkout process because you have to take the time to input something you know," explains Aiden Foley, engineering lead for authentication at payment service provider Stripe. These identifiers can also have the effect of flagging genuine activity as fraudulent. Shikiar points out that forgetting a password is something which every online shopper has experienced, while two-factor processes often fail if the information doesn't match with records completely and perfectly.

"The methods that most businesses use to stop fraud can turn away genuine customers. If an order placed by a genuine customer is declined, they may not have the patience – or time – to contact the merchant," explains Ajay Bhalla, president for cyber and intelligent solutions at Mastercard.

In June 2022, Stripe launched delegated authentication for its clients. Any customer using a card issued by Wise (formerly TransferWise) is now able to authorise payments in a select number of vendors' mobile checkouts. Early adopters include Nando's, Deliveroo and TikTok. Stripe reports a 7% improvement in conversion for customers using delegated authentication at checkout – a figure that shows "enormous promise for a broader roll-out with more card issuers", according to Foley. "Delegated authentication is a win-win. The consumer gets an easier checkout flow, the merchant gets more revenue as checkout conversion increases, and the ecosystem retains the SCA benefit of reduced fraud."

> **The methods most businesses use to stop fraud can turn away genuine customers. If an order placed by a genuine customer is declined, they may not have the patience – or time – to contact the merchant**

While the benefits seem clear, there are still a few examples of seasoned players using delegated authentication. Bhalla says vendors don't, however, need to do extensive work to implement delegated authentication. "As with any emerging technology, there is work to do ahead of an integration. But retailers can use existing investments in authentication, such as tokenisation or EMV's Three-Domain Secure system, to streamline the integration process and reduce the costs and time associated with it.

"We expect to see growing adoption by retailers keen to improve conversions and reduce risk. That said, the technology is evolving and we expect widespread and faster adoption as standards evolve."

Shikiar adds that, to his knowledge, there have been no examples of fraud in the admittedly small sample of delegated authentication transactions.

He doesn't think businesses need fear large-scale security risks. "If you look at these payment networks and their history of managing secure transactions and payments, the merchant's risk is mitigated."

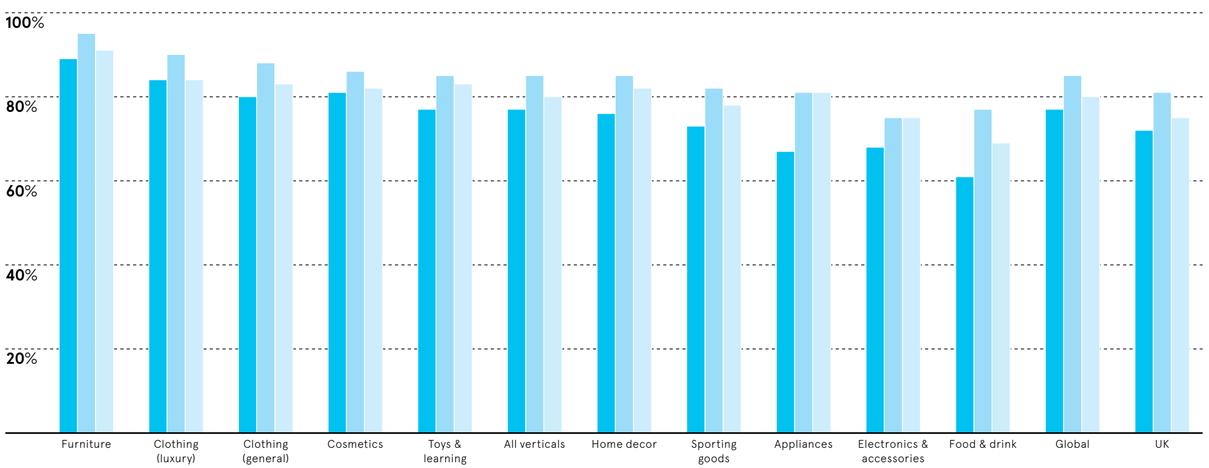
Foley cites card issuers as the biggest barrier to wider adoption. Historically, these parties would bear the greatest burden in authentication, as they could be held responsible by both merchants and cardholders in the case of fraudulent activity. He thinks it is now their responsibility to cede control in favour of new authentication technologies and to help users understand their benefits.

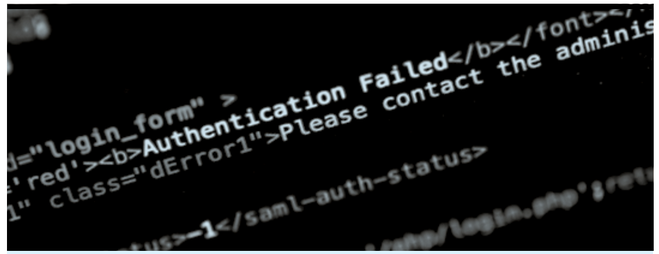
"The challenge is that card issuers need to be comfortable with delegating their responsibility for authenticating transactions. That, and the fact that the industry as a whole needs to help consumers understand the value of biometric authentication."

**FINDING WAYS TO SMOOTH THE CUSTOMER JOURNEY IS VITAL**

Salesforce, 2022

Percentage of online shopping carts abandoned before a purchase




## Using AI to know your customer

The know-your customer (KYC) processes used by banks and other financial institutions are now more strictly regulated since PSD2 arrived here in the UK and EU last year.

Financial services providers are required to hold a knowledge-based signifier such as a password, plus either a biometric identifier or a possession-based security check, normally via a two-factor authentication process on a specific device. This is typically carried out periodically when customer information is changed or if there is a threat to account security.

This as-and-when approach brings its own problems, however. "Relying on periodic KYC checks carries inherent risk," says Chris Foye, market planning director at LexisNexis Risk Solutions. "Customers' circumstances do change and can affect their level of risk. This potentially results in a risk residing within the business for a significant time without the compliance team being aware of it and without mitigating actions in place."

Increasingly, then, KYC will become a constant process of verifying a customer's identity through different touchpoints which are built into a bank or financial institution's digital framework.

Richard Hoehne is senior partner for risk, fraud and financial crimes at IBM. He says that a truly holistic KYC solution must focus on three key elements: identifying and stopping criminal activities; ensuring compliance with regulations; and not impinging on the customer experience. "It's critical that KYC due diligence is consistently and universally applied across all aspects of a bank and evaluates information continuously to assess risk and initiate follow-up when risky behaviour is observed," he explains.

The answer could well be AI. Research by NTT Data shows that 57% of banks are using AI in their KYC processes. Hoehne describes how this technology's role is twofold. It offers banks the opportunity to spot suspicious activity within an account. And then it provides greater security at the point of access through functions such as keystroke analysis or voice recognition.

"AI-based technology has the power to fundamentally change how we approach KYC and identify risky customers. Finding and stopping fraud and money laundering is a study in behaviours and relationships," Hoehne says. "We can use AI to write rules, interpret documents, spot abnormal behaviours and more. The more we can apply this technology, the better our chances of stopping the bad guys."

But he points out that implementing AI security systems alone won't be enough to stop malicious actors from breaking through the defences. "Keystroke detection and other advances by themselves will not stop criminal activities. When combined with AI scoring and intelligent decision-making, it can have a significant impact."

Commercial feature

# Finding the identity verification sweet spot

Payment service providers are searching for the balance between security and experience

Online payment service providers (PSPs) have a balance problem.

On the one hand, platforms are in an arms race with fraudsters who want to cheat security measures, take over accounts and steal money. On the other, PSPs want to onboard legitimate customers quickly and conveniently and provide ongoing experiences that are as near to frictionless as possible.

That's a tough balance to strike because the more security steps there are, the more friction customers face. The more steps removed, the bigger the fraud risk.

So, what's the sweet spot between security and experience? New research from Trulioo, a leading global identity verification company, provides answers to some of the PSP sector's most pressing questions.

**The pandemic effect**

The right balance isn't a constant, and it isn't the same for everyone. Priorities differ between jurisdictions and platforms, and even from one year to the next.

The pandemic shifted the dial in favour of security. The Trulioo consumer and business research found that 73% of online payment service customers consider security more than they did three years ago, and 52% are less trusting of online brands.

COVID-19 accelerated the transition to digital commerce, and bad actors seized the opportunity. An explosion of information around online safety prompted consumers to prioritise security over convenience.

That remains today. More people transact online, but they're on high alert when engaging with online companies. That has huge implications for PSP platforms.

**Consumers want reassurance**

The biggest implication might be that, if a platform doesn't provide reassurance, customers will go elsewhere. People want to feel protected at the moment they open an account and through the customer journey.

That's made them more tolerant of friction. The research found that 78% of online payment service customers say they are comfortable with identity verification taking longer or involving more steps.

For years, smooth, fast, convenient customer experiences have been the digital dream. Today, customers want to be safe, even if that makes online life a little bumpier.

The Trulioo research goes further. It found that security, at 79%, was the top factor for PSPs in building trust with customers through identity verification. Creating accounts with as few steps as possible came in fourth at 48%.

So has security won the day, with experience only a secondary consideration? Well no, it isn't that simple.

**The right kind of friction**

As the research found, consumers are tolerant of security measures, to an extent. But they like security that isn't overly burdensome. PSP customers in the research had similar expectations.

"Consumers will accept friction, but it has to be the right type of friction," says Michael Ramsbacker, Trulioo chief product officer. "That means it has to be at the right level and at the right time. Platforms that get that balance wrong risk losing customers to rivals."

PSPs can't necessarily match an iPhone for ease of identity verification, but they can provide fast, smooth, transparent digital experiences. If setting up an account becomes too onerous, consumers might walk away.

**Getting the balance right**

Coexistence requires compromise, which is why PSPs often struggle to find the sweet spot between security and experience.

The Trulioo research shows how difficult it is. More than half (57%) of PSPs have added more identity verification steps to counter new security risks. At the same time, 40% removed or simplified steps to speed up customer onboarding.

That illustrates the industry's dilemma. For Ramsbacker, it's easy to see why. "PSPs are balancing a range of factors," he says. "They want to onboard as many good customers as possible. They've got fraud teams trying to keep bad actors out. They've got compliance regulations to think about. And on top of it all, if they're operating internationally, there might be big differences in customer experience, acceptable methods of customer identification and applicable regulations from one country to the next."

PSPs are clearly being pulled in multiple directions in their quest for the most secure, convenient and globally compliant experience. What's more, as technology advances, regulations evolve and fraudsters react. It's no wonder more PSPs are looking for help.

**Creating strategic partnerships**

So, how can PSPs provide exceptional experiences and keep customers safe? For a start, they can try to understand the customer journey in detail, starting with onboarding. They can then use that information to create an identity verification strategy that deploys a well-considered mix of passive and active anti-fraud techniques.

While passive measures are largely friction-free, active measures inconvenience customers to some degree. Getting the timing and sequencing of active verification right can be the key to keeping customers. Typically, PSPs start with low-friction activities, such as entering a name, birth date or national ID number. High-friction activities, such as a document scan, might be reserved for high value transactions.

As customers progress on their journey, unusual activity should then prompt additional security measures.

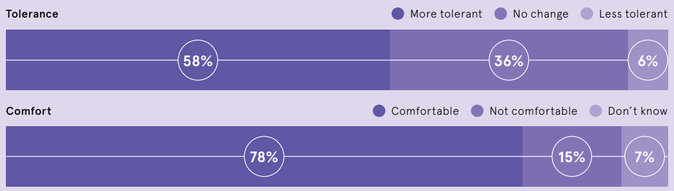
Data-driven, automated and accurate processes can help PSPs maximise the number of legitimate customers getting through and bad actors locked out. That complexity increases for PSPs operating internationally.

That's why more PSPs are turning to Trulioo as a strategic partner in identity verification. Trulioo leverages industry-leading identity verification tools with access to hundreds of data sources worldwide.

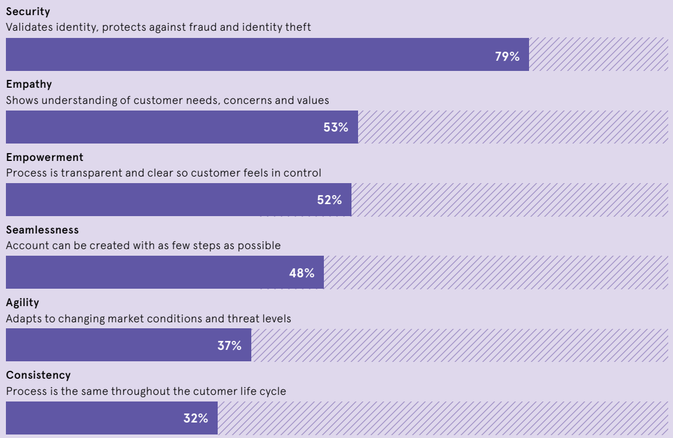
The company offers expertise to monitor the threat landscape, tailors identity verification strategies for PSPs' unique needs, and provides coverage around the world.

Trulioo can help PSPs find the identity verification sweet spot and strike the balance between robust security and smooth digital experiences.

**CONSUMERS ARE MORE TOLERANT OF IDENTITY VERIFICATION THAN THEY WERE TWO TO THREE YEARS AGO AND ARE COMFORTABLE WITH THE PROCESS TAKING LONGER**




**PAYMENT SERVICE PROVIDERS ARE PRIORITISING SECURITY TO BUILD CUSTOMER TRUST IN THEIR IDENTITY VERIFICATION PROCESSES**




Trulioo, 2022

> Trulioo can help PSPs find the identity verification sweet spot and strike the balance between robust security and smooth digital experiences

**For more information, visit trulioo.com**

Trulioo



TECHNOLOGY

# What blockchain means for personal data

Could a blockchain-based ecosystem strengthen the security of digital ID and future-proof the next generation of online interactions?

Emma Perry

Perhaps the most valuable asset we have online is our identity. It allows us to buy and sell items, even open a bank account. It's understandable, then, that people might have qualms about trusting their identifying personal data to blockchain (the technology behind crypto), which has experienced more than $1bn (£840m) in fraud since the start of 2021.

Trust, though – along with greater security – is the object of the exercise. Blockchain-based digital ID is based on the principle of self-sovereign identity (SSI), whereby users can share selected information with vendors or service providers instead of their entire identity. The analogy is of a person walking into a bar and presenting a trusted credential that proved that they were of legal age to buy an alcoholic drink – instead of presenting an ID card that might include their name and address details.

SSI means that the interacting parties know they can trust each other because they can see the key information in question. And blockchain-based digital ID could make this a reality.

"This is significant because currently there isn't a way for businesses online to interact with contractual trust in a peer-to-peer way that isn't intermediated by a third-party login service," says John Jordan, executive director of the Government of British Columbia's Digital Trust Service, which is starting to implement blockchain-based ID systems for citizens and local businesses.

"Blockchain presents the important opportunity to have confidential friendships and business partners on a foundation of trust."

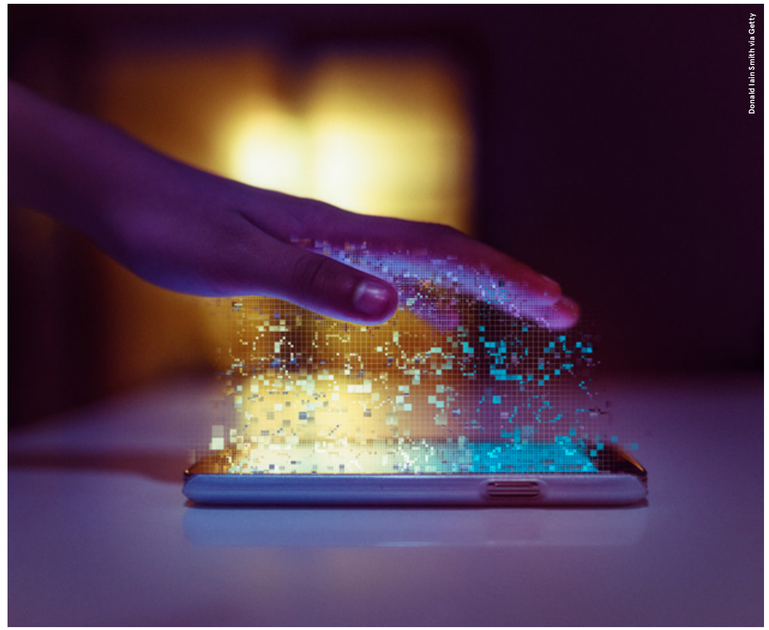
As well as trust, one of the main benefits of a decentralised blockchain ID would be interoperability. The current digital identity experience is fragmented; there are multiple platforms and logins globally. Verifying credentials across these platforms is both costly and time-consuming. "Interoperability across chains can result in a bigger ecosystem, allowing businesses to reach out to a wider audience," says David Palmer, visionary and global platform innovator and blockchain lead at Vodafone Business. "Blockchain can act as a 'network of networks' to achieve this."

What's more, with interoperability will come automation, allowing companies to verify user data across industries without needing to contact different sources or report to multiple regulatory bodies. The Government of British Columbia has implemented an automated system for business licensing rights via a verified credential. As Nathaniel Amann-Blake, assistant deputy minister at Government of British Columbia, explains: "Blockchain has been critical in improving efficiency, automation and trust in this sector, where there has always been a large and changing regulatory landscape."

Automation will also become increasingly valuable if digital spaces such as the metaverse catch on. "If, in the future, we will have digital personas crossing into different digital platforms, there will need to be full automation of ID verification, as there won't be people around to verify things at each digital border," observes Palmer.

There is also a case to be made for blockchain-based ID reducing fraud. Most digital IDs are stored on centralised databases, making them a honey pot of information vulnerable to accidental exposure or deliberate theft. "As blockchain IDs allow companies to hold only specific pieces of data, it's almost impossible to be hacked," says Daniela Barbosa, executive director at the Hyperledger Foundation, an open-source creator of distributed ledgers. "It's also more efficient and cost-effective, as you are processing and storing less data," she adds.

Unsurprisingly, there are implications too for how businesses might look to monetise customer data.



Donald Iain Smith/via Getty

> Interoperability across chains can result in a bigger ecosystem, allowing businesses to reach out to a wider audience

"Decentralised SSI gives customers the ability to opt out of certain types of data being shared with a company, for example when they buy something. Customers may now look for some sort of reward for sharing their data. There is a real opportunity here for businesses to reshape their business models to see how they can add value from this," says Palmer.

It will all come down to business leaders thinking carefully about the data collected and the implications of that for the entire business.

For Taylor Monahan, global product lead at crypto-wallet-provider MetaMask, the key is not to default to accepted norms, such as offering sign-on with a single button, but to "think about the relationship with customers" and to use this new technology to "unlock new capabilities for users and to empower them".

That means now is the time for business leaders to start investigating real use cases for blockchain-based ID. Many of the current examples of implementation are no longer pilots but genuine replicable models. "What we need to do now is to understand the value of these new business models," claims Heather Dahl, CEO of Indicio.tech, which has partnered with Google to offer a trusted digital ID ecosystem for companies via the Google Cloud marketplace. "This could even be within a business to overcome departmental silos," she adds.

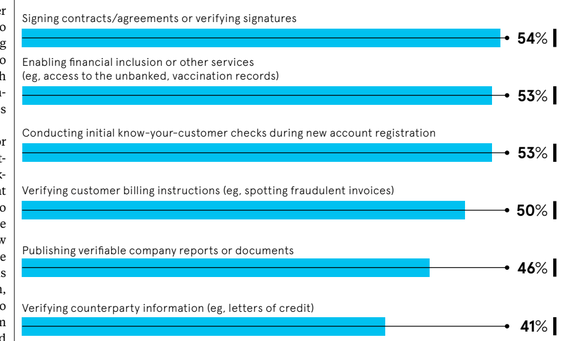
Of course, the adoption of a blockchain ID system would also require significant employee engagement across departments, from legal to marketing to HR, to meet the necessary know-your-customer rules, privacy regulations or Web3 standards.

Andrew Thomson is a digital ID, insights and blockchain analyst at Janssen Pharmaceuticals, part of Johnson & Johnson. He stresses the importance of building and testing systems to ensure the right level of privacy, transparency and security. "While blockchain might not be corrupted technologically, without the right governance and change-management controls in place, other areas may fall short," he warns.

By 2030, the ID2020, a UN alliance of industry, government and academia, aims to achieve universal digital ID using blockchain and, so far, the role of government has been key. The development of the existing use cases has mainly been the result of collaboration between open-source communities and governments worldwide. Thomson thinks blockchain ID can be used to help people – with voting or social security. "But government must support whatever solution is finalised, to gain the adoption and trust industry needs," he says. Monahan too is optimistic. "It's important to think openly about the potential of blockchain technology and ID today. There's unimaginable value when people are empowered and have the confidence and space to innovate."

**THE FINANCE INDUSTRY IS EXCITED ABOUT BLOCKCHAIN-BASED ID**

"Which of the following applications [for blockchain] would offer the most value to your organisation?" (Survey of financial services executives)

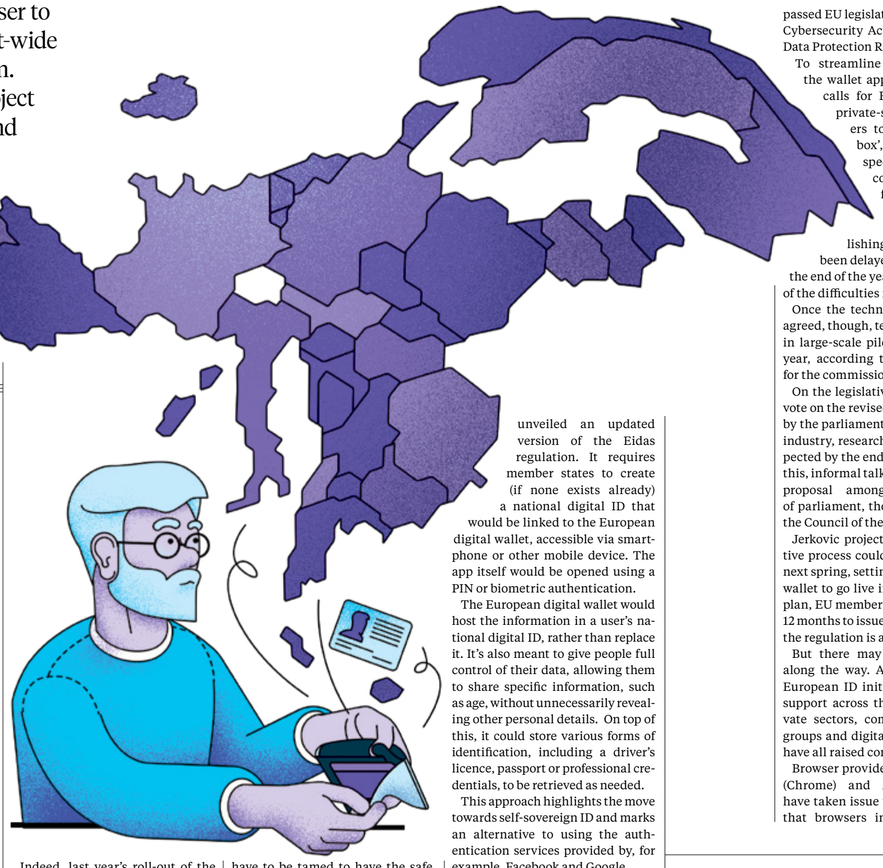



Deloitte, 2021

PUBLIC SECTOR

# Going big: the EU's digital identity wallet

The EU is moving closer to rolling out a continent-wide digital identity system. But the ambitious project still faces technical and legislative obstacles



Mark Walsh

The abrupt shift to a more digital-centric life during the pandemic meant going online for everything from food shopping to doctor's visits to renewing a passport. The sharp rise in demand for digital services underscored the need for a convenient, widely accepted way for people to prove who they are online.

For the European Union's 450 million citizens, that process is poised to get easier with the introduction of a pan-European Digital Identity wallet app that would allow users to access public and private services in their own countries and across the bloc. The digital wallet would serve as proof of identity to, for instance, open a bank account, enrol in a university, rent a car or file tax documents.

Already, 14 of the EU's 27 countries, accounting for 60% of the total population, have some type of national digital system but not all can be used cross-border. And that still leaves millions without any form of digital identification.

"I think that we will see an increase in demand for robust, secure and easy-to-use digital identity tools. Europe wants to be at the forefront of the development and use of the digital identity," observes Romana Jerkovic, an MEP representing Croatia who also serves on the European Parliament's committee on industry, research and energy.

Indeed, last year's roll-out of the Covid-19 health certificate app – the so-called vaccination passport – helped to ease travel in the EU during the pandemic and provided a glimpse of what the European digital ID could be when launched, if as planned, in two years.

But the ambitions here are on a grander scale, with daunting policy and operational challenges that will have to be tamed to have the safe, seamless digital ID system the plan envisions EU-wide.

The blueprint for a European digital ID began in 2014, when the EU adopted legislation for electronic identification and trust services (Eidas) among its member states. Prompted by the pandemic-fuelled surge in digital operations, in June 2021 the European Commission unveiled an updated version of the Eidas regulation. It requires member states to create (if none exists already) a national digital ID that would be linked to the European digital wallet, accessible via smartphone or other mobile device. The app itself would be opened using a PIN or biometric authentication.

The European digital wallet would host the information in a user's national digital ID, rather than replace it. It's also meant to give people full control of their data, allowing them to share specific information, such as age, without unnecessarily revealing other personal details. On top of this, it could store various forms of identification, including a driver's licence, passport or professional credentials, to be retrieved as needed.

This approach highlights the move towards self-sovereign ID and marks an alternative to using the authentication services provided by, for example, Facebook and Google.

Large platforms enable easy access to third-party services online but aren't necessarily accompanied by sufficient privacy or data protection. To that end, the commission's proposal for the digital wallet promises high-level security, with member states required to meet strict privacy and data protection requirements in compliance with recently passed EU legislation, including the Cybersecurity Act and the General Data Protection Regulation.

To streamline the building of the wallet app, the project also calls for EU countries and private-sector stakeholders to develop a 'toolbox', setting technical specifications and common standards for the project. The fact that the timeline for publishing the toolbox has been delayed from October to the end of the year illustrates some of the difficulties involved.

Once the technical framework is agreed, though, testing of the wallet in large-scale pilots can start next year, according to a spokesperson for the commission.

On the legislative front, an initial vote on the revised Eidas regulation by the parliamentary committee on industry, research and energy is expected by the end of this year. After this, informal talks can begin on the proposal among representatives of parliament, the commission and the Council of the EU.

Jerkovic projects that the legislative process could be completed by next spring, setting the stage for the wallet to go live in 2024. Under the plan, EU member states would have 12 months to issue their wallets once the regulation is adopted.

But there may be more bumps along the way. Although the pan-European ID initiative has general support across the public and private sectors, companies, industry groups and digital rights advocates have all raised concerns.

Browser providers such as Google (Chrome) and Mozilla (Firefox) have taken issue with the mandate that browsers include additional trust certificates, which provide a certified guarantee of who is behind a website. They argue that these digital certificates would be a great deal less secure than their existing means of authenticating websites and would require significant web infrastructure work to accommodate the proposed changes in vetting websites.

Companies and trade groups have also pushed back against the Eidas regulation's requirement for private sector parties in key industries, such as banking and financial services, transport, telecommunications and health, to accept the EU digital identity wallets. That provision also extends to "very large online platforms".

In public comments submitted in response to the European ID plan, Apple suggested that integrating the wallet would impose significant costs and workloads on private parties while also putting startups and smaller companies with competing digital identity services at a disadvantage. (Apple has its digital wallet in its iPhone.)

There are qualms on the public-interest side too. Among them is the proposed requirement for EU states to include unique identifiers – alpha-numeric strings – in digital IDs.

Campaign group European Digital Rights maintains that such identifiers could be used as so-called super cookies to track users' daily activities that require the ID wallet. The group also warns that the feature might be unconstitutional in Germany and run counter to current administrative practices in both Austria and the Netherlands.

Despite this, Thomas Lohninger, vice-president of European Digital Rights, observes that there are signs in the current Czech presidency of the Council of the EU of a shift towards record-matching as a less invasive technique for authentication. He argues that the European ID system ought to embrace the same principles of unobservability and privacy by design – the concept of building data protection into technology design – which were successfully incorporated in the development of the EU's Covid-19 certificate.

"We have proved that this can work," says Lohninger, noting that the certificate was also developed at "lightning speed" compared with other big EU projects.

None of this is lost on Jerkovic. As rapporteur for the European Parliament's committee on industry, research and energy earlier this year, she recommended amendments to the ID proposal, such as for the wallet to ensure cybersecurity and privacy by design. It should, she suggested, reflect the "once-only principle", so that users don't have to provide the same data twice to public authorities.

But Jerkovic also points out the differences in scope and sophistication between the projects: "The Covid-19 certificate helped us to lay the groundwork on both the regulatory and technical sides. But, of course, building a pan-European digital ID framework is a much more complex task. It targets many more possible use cases."

In short, maybe it would be wise not to expect lightning to strike twice.

> **The Covid-19 certificate helped us to lay the groundwork, but building a pan-European digital ID framework is more complex**

> **Once the technical framework is agreed, testing of the European wallet in large-scale pilot projects can begin next year**

**53%** of Europeans don't feel in control of their data

**3%–13%** The boost to a country's GDP by rolling out fully digital ID

**50%** of which is expected to accrue directly to individuals

McKinsey, 2019





Commercial feature

# Continuous trust: a shot in the arm for user experience

Entire customer journeys are taking place within advanced digital ecosystems where trust is easier to break and harder to build. How can businesses strike the right chord?

For the first time, 2021 saw successful fraud attempts outnumber those prevented. This leap in cases brings the severity of current data breach concerns into sharp focus.

More than ever, leaders are tasked with balancing trust, a cornerstone for building loyalty and enhancing brand reputation, and customer experience. The convenience economy is thriving and catering to time-hungry customers while delivering secure connections is crucial for longevity in highly connected online environments.

Joe Burton, CEO of digital identity company Telesign explains: "As security has improved, the process for the consumer has become more elaborate and complicated; you have a name, you have a password. Now you need a longer password. Now you have to answer five challenge questions". Enhanced security, a necessity in the ever-growing digital world, comes with a lot of potential friction for customers.

"In balancing security and user experience, there cannot be a trade-off. But how do we create an experience that has the appropriate amount of friction, the appropriate amount of assuring you that there is security, and still make it easy enough?"

With fraud becoming increasingly common, costly, and complex for businesses to manage, simpler solutions seem to be a hit with consumers. Two-factor authentication (2FA) and multi-factor authentication (MFA) options, often involving the elusive SMS one-time passcode, are effective means of mitigating account theft and fraud. These tried-and-tested techniques come exceptionally close to nailing the 'trust versus friction' sweet spot.

Going forward, Burton advocates a departure from existing methods of customer identification. Rather than requiring customers to repeatedly prove their authenticity through interminable login rituals and security questions, he envisages a reciprocal digital relationship where companies recognise the customers within their online spaces from their behaviours, actions and patterns.

"It's a model of continuous trust, creating a positive real-world experience in the digital world, where we are looking at a variety of factors in the background, but only asking you questions as you need them," he says. Before making a purchase or transferring money customers are interacting in a digital space that feels personal, providing reassurance and connection with the brand identity. Burton continues: "It's about how we appropriately model that in the digital world to maintain continuous trust across the entire digital consumer journey."

Most brands incorporate trust as a core pillar of their value propositions in some way, shape or form. But advancements in digital infrastructure and the threats that come along with them mean businesses need to take stock of what this means in the context of an expanding digital economy.

The challenge today for companies like Telesign is protecting people. Tomorrow's challenge will be protecting devices and machines as the practical applications for digital identity become more mainstream. For example, the UK's proposed digital ID scheme aims to make digital identities as secure as official identity documents. Available via a phone app or website, these could hold equal weight to passports and driver's licences.

With this uptick in the prevalence of digital identities, continuous trust will be even more critical, says Burton. "Someone could be checking out online, but those checks still need to happen in the background. Ensuring that they are who they say they are, in a location where they are likely to be," he says. "Using those historical behaviours and data points, it's easier to spot unusual activity and prevent anything suspicious from becoming a problem."

Ultimately enhanced digital trust profoundly impacts how consumers perceive and engage with a brand. Users are more likely to recommend a brand they implicitly trust, but customers who are required to jump through too many hoops to be assured complete security may reach a point of no return. No matter how wonderful the brand proposition or the product, convenience and compliance must be in lockstep. For Burton, the implications are clear: "If we ever suspect that a brand is abusing our trust in them, if we suspect they're not safeguarding our personal information, we move from advocate to adversary very quickly."

> **In balancing security and user experience, there cannot be a trade-off**

**For more information visit telesign.com**

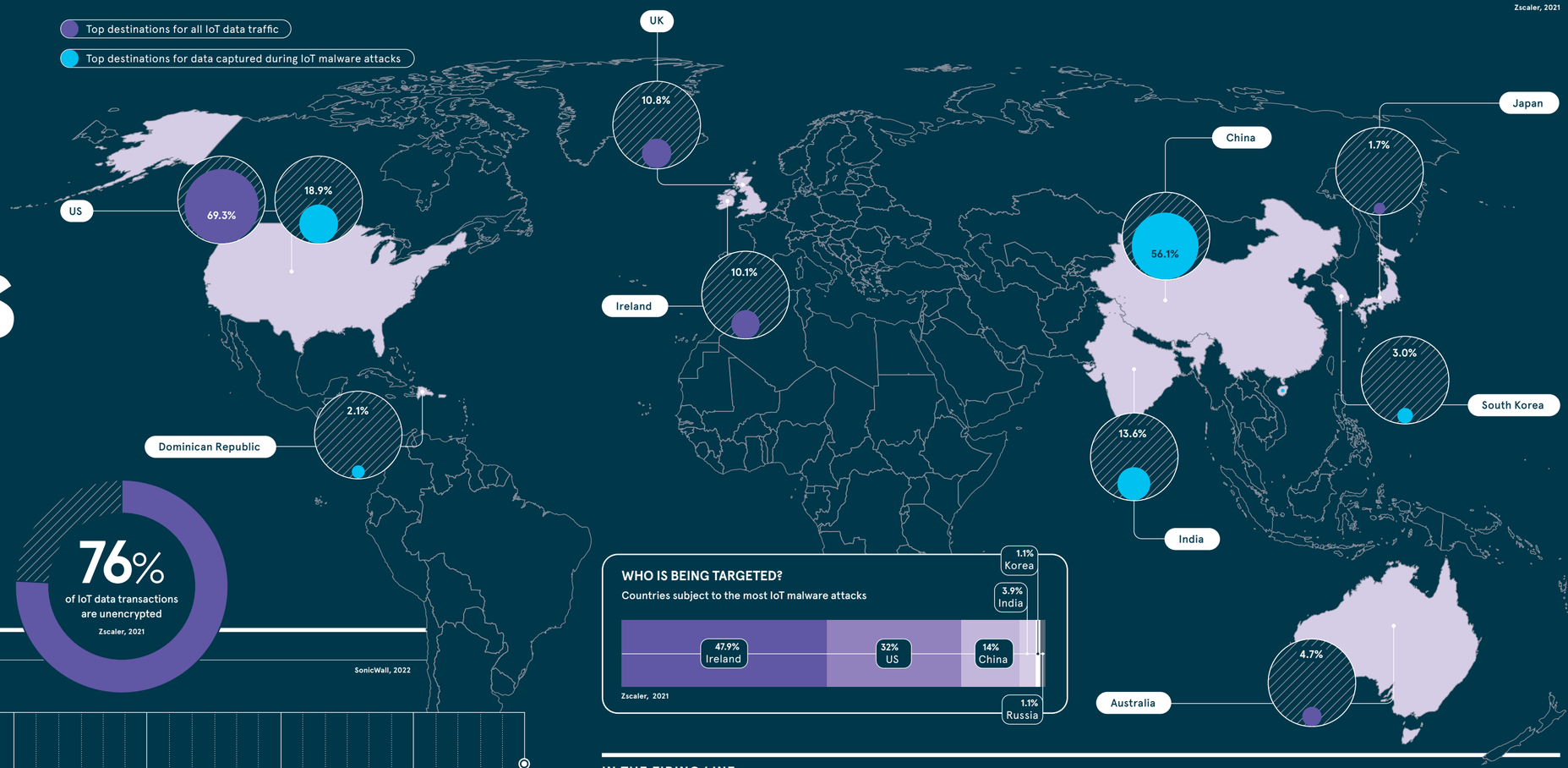
telesign

# MALWARE AND THE INTERNET OF THINGS

As more and more devices become 'smart', we're trusting huge amounts of personal and business data to the cloud, often without realising it. It all means that those individuals and businesses which are lagging on cybersecurity are putting themselves at risk of falling victim to IoT-based malware attacks. This is particularly true for SMEs, which might not have the resources to dedicate to this problem, and for those countries where SMEs account for a bigger proportion of the economy. Tighter security around user authentication, passwords and up-to-date security protocols, then, will be an essential investment in the years to come

## WHERE'S IT ALL GOING?

Zscaler, 2021




**76%**
of IoT data transactions are unencrypted
Zscaler, 2021

## WHO IS BEING TARGETED?

Countries subject to the most IoT malware attacks




Zscaler, 2021

## A GROWING PROBLEM

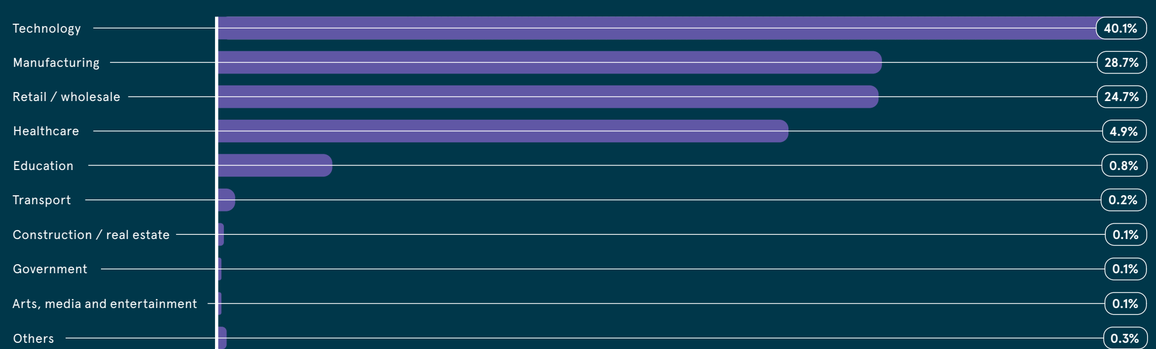
Number of recorded IoT malware attacks worldwide (millions)

SonicWall, 2022


## IN THE FIRING LINE

Share of recorded IoT attacks, by industry

Zscaler, 2021



TRAVEL

# Lessons from airport biometrics

Air travel was one of the first sectors to deploy biometric tech across the entire customer journey. What, then, can airports teach other travel, retail and payment businesses?

**Paul Sillers**

For some time, airports have been using biometrics to identify passengers as they pass through the terminal checkpoints, from check-in kiosks to boarding gates. The idea is to speed people through the bottlenecks and get passengers into the retail and restaurant areas, where airports make a third of their revenue.

Now, though, airports are working to make the customer journey even more seamless.

The Star Alliance biometrics platform enables members of Lufthansa's Miles & More frequent flyers programme to pass through designated checkpoints at Hamburg, Vienna, Frankfurt and Munich airports without producing their travel documents. The passenger's face is captured by cameras installed at gates and fast lanes, which automatically open once matched with the passenger's stored image. Star Alliance aims to have half of its 26 airline members using biometrics by 2025.

"With the roll-out of Star Alliance Biometrics, the benefits of biometric identification will be extended from a single airline or journey to a vast network of airlines," says a spokesperson for the Société Internationale de Télécommunications Aéronautiques, which supplied the underlying technology.

Of course, a fundamental aspect of airports' uptake of biometrics is the fact that 75% of passengers are reportedly willing to use this technology in place of physical passports and boarding passes. More than a third have already experienced the use of biometric identification in their travels, with an 88% satisfaction rate, according to a recent Iata study.

"Passengers want improved convenience throughout their trip," says Nick Careen, Iata's senior vice-president for operations, safety and security. "Digitalisation and the use of biometrics to speed up the travel journey is the key."

Robin Tombs, co-founder and CEO of digital identity and biometrics company Yoti, has a similar message: "After Covid struck, we worked with Heathrow and Virgin Atlantic to introduce pre-flight Covid tests for crews. Since then, there has been a lot of movement towards digital services. Above all, customers want privacy and convenience – and biometrics ticks both boxes."

But data protection remains a concern. As many as 56% of passengers worry about data breaches and want clarity on who their data is being shared with. Corporations are already factoring in the potential cost of remedying identity breaches; global business consultancy Gartner predicts that lawsuit costs linked to biometric information and cyber-physical systems will have exceeded $8bn (£6.7bn) by 2025.

So, what comes next? Can other sectors emulate the roll-out of biometric tech at airports? And can they get consumers on side with the offer of greater convenience and effective data security?

Joe Palmer is chief product and innovation officer at iProov, a global player in biometric authentication. According to him, it is already happening. "Biometric tech is not unique to the airline industry. It can be applied to eliminate check-in bottlenecks for other forms of travel, including trains, cruise ships, car hires and more," he says.

Last winter, iProov partnered with Eurostar to trial SmartCheck, a fast-track service that uses iProov's technology to biometrically scan travellers while guarding against identity theft and cybercrime. Business Premier and Carte Blanche passengers were invited to scan their identity documents using their smartphones before arriving at the station, then completed a biometric face scan to verify that they were the holder of the identity document. Biometric verification was then linked to their e-ticket.

"The trial showed that there is demand for convenient, secure travel, and conversations are ongoing about the next iteration of this programme," Palmer says.

Elsewhere, domestic rail networks are also embracing the advantages of biometrics. Vodafone recently worked with Spanish rail administrator Adif at the Maria Zambrano station in Malaga to implement a pilot for an intelligent railway station. Various scenarios for customer and employee access through the station were explored to evaluate the benefits of combining biometrics with Vodafone's 5G coverage.


> **Since Covid struck, there has been a lot of movement towards digital services. Customers want privacy and convenience – and biometrics ticks both boxes**

Equally, with consumers venturing into the real world following lockdowns, retailers are looking to improve journeys of a different sort – through stores on the high street.

Amazon's Fresh stores use a range of optical technologies to biometrically track customers as they take groceries from the shelves. To check out, customers simply leave the store with their chosen goods. Alternatively, they can scan a QR code with their Amazon app or use Amazon One to biometrically scan their palm. Tesco offers a similar set-up with its checkout-free GetGo stores in London and Welwyn Garden City. Realistically, though, few retailers have the budget or technological prowess to retrofit such systems in existing shops.

This barrier to widespread adoption could be an opportunity for payment providers such as Mastercard, which has recently launched the Biometric Checkout Program. The firm says it's aiming to create a "technology framework to help establish standards for new ways to pay at stores of all sizes, from major retailers to small family businesses".

Mastercard's first biometric installation was installed across five St Marche supermarkets in São Paulo in May. Once consumers had registered their face and payment information through the Payface app, they simply had to smile to pay at the checkout. Further implementations are now planned across the Middle East and Asia, and the system can also be integrated with loyalty programmes so that personalised deal alerts are sent to customers.

The impetus behind the roll-out of this technology comes from changing consumer behaviour, especially among generation Z. These savvy customers are demanding a smarter approach to embedding biometrics.

"Rabobank is a great example," says iProov's Palmer. "They were losing younger customers by asking them to go into a branch to upgrade from a junior account to an adult one. But now, by using biometric scans in their mobile app instead, Rabobank is retaining those customers and encouraging young digital users."

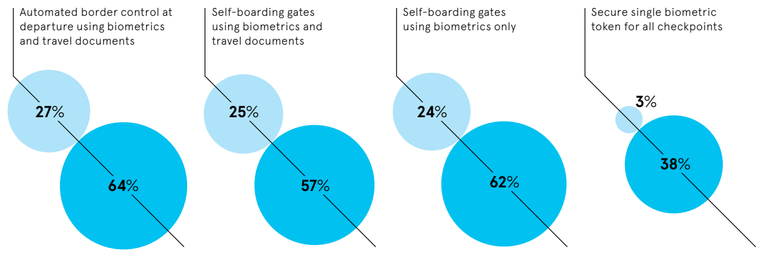
While biometrics has strong roots in air travel, its next steps may be where industries intersect. Since September, passengers boarding domestic flights at 14 Korean airports can confirm their identity with palm vein-based biometrics, thanks to an initiative between the Korea Airports Corporation (KAC), nine financial institutions, and the Korea Financial Telecommunications & Clearings Institute. Under the scheme, passengers who have registered their palm vein data and smartphones at participating banks can complete the identification process at designated boarding gates in a faster, more efficient way. One airport has reported that the journey from check-in to baggage drop-off and identification now takes just five minutes.

With KAC president Yoon Hyeong-jung saying there are plans to "expand the service to duty-free shops, unstaffed vending machines, and for check-in procedures", it looks like the future is very much on its way.

**AIRPORTS ARE INVESTING HEAVILY IN BIOMETRICS**

Société Internationale de Télécommunications Aéronautiques, 2021

Percentage of airports with implemented or planned biometric ID systems






Commercial feature

# Credential-less is more: why password rotation doesn't mean 'zero trust'

Biden's endorsement of compulsory zero trust access management and quantum-safe cryptography is shifting the C-suite's cybersecurity agenda for the US government and global businesses

With cyberwar becoming more sophisticated, President Biden mandated that all US federal agencies adopt a zero-trust access security model early last year. As a result, the world is charting a course to a new system of continuous verification, credentials management and mandatory encryption of digital communications, regardless of whether the user is inside or outside the network.

Miikka Sainio, CTO at defensive cybersecurity company SSH, believes that the White House's actions indicate a step change in the popularity of zero-trust principles across the board. "It's significant that they mandated it not just for IT infrastructure but also for critical infrastructure like water and electricity," he says.

In May 2021, Biden encouraged government agencies to mitigate the security risks posed by quantum computing, which could one day be used to decrypt sensitive data that today's computers have encrypted retroactively. This sentiment was echoed in the response from heads of executive departments and agencies worldwide.

This move is a striking reminder for business leaders that static secrets for access control and quantum computing threats should be on their radars. Encrypted critical traffic is being captured and recorded today. So IPR, account numbers, credit card details, ID codes and health information that are currently protected are all at risk of being revealed in the future. This could spell staggering financial losses, reputational disaster, and heavy fines for firms and other establishments that miss the mark.

Preparing for the quantum threat is not mere future gazing. Tools that address tomorrow's quantum computing threats are already available. Quantum safe (or post-quantum) cryptography is a prime example of preventing data from being decrypted by quantum computers in the years to come.

**Optimising credentials management**

For convenience and continuity, colleagues or external organisations may create universal or shared password credentials for multiple company accounts. Add unsecured messaging apps and personal devices into the mix, sprinkle in a global shift to the cloud, and businesses have a recipe for a security breach.

Some companies have turned to privileged access management (PAM) tools to vault and rotate passwords and ensure their employees use them responsibly. However, these often fail to fully support the management of other vital credentials like SSH keys.

Passwords have the potential to grant access to all manner of things, from credit card data to medical and tax records, intellectual property rights, CI/CD pipelines, cloud servers, firewalls and network devices. But SSH keys almost always grant access to these critical systems.

DevOps teams, for example, use SSH keys to commit code changes to code repositories. "The developers have uploaded their public keys to the repository and authenticate with their private key, which is on their laptop but without a recognisable link to the user," says Sainio. "Now, what happens if somebody steals the private key? They will have access to the code repository that contains company IPR. What's more, there's no way to verify who is using the key, as keys can be copied, and they never expire."

Running application-to-application connections within cloud or hybrid environments and frequently hidden in repositories or behind other servers, SSH keys often constitute 80% of all credentials in large organisations. At best, most PAM solutions discover only 20% of keys, leaving thousands of them scattered across the IT environment at a given moment.

SSH key and password adoption are booming in line with the rise in internal and external users accessing critical cloud assets.

There are issues on the operational technology side too. Rami Raulas, vice president for EMEA at SSH, says that many remote connections to factories, plants and power stations, which are needed to enable industry 4.0, have created security holes.

"When you physically go to a manufacturing site, power plant or water facility, someone checks your identity at the gate; you go in escorted and do your job", he explains. "In the digital world, your suppliers are climbing over the fence, there's a hole in it, they have underground tunnels, and you have no idea who's coming in or doing what."

**Realising zero trust and quantum-safe access management**

Reaching the level of defensive cybersecurity that SSH proposes starts with recognising the need for coherent risk mitigation strategies. For businesses, centralising the management of all keys and passwords could allow for greater visibility, accountability and command over credentials.

Without overcomplicating the matter, SSH's Zero Trust Access Management provides organisations with enhanced centralisation and control by reducing the number of passwords and keys floating about the IT and OT environment. This could mean transitioning to efficient passwordless and keyless zero-trust architectures in connected businesses.

> **In the digital world, your suppliers are climbing over the fence ... they have underground tunnels, and you have no idea who's coming in**

The same protocols needed to connect people and machines are still used, but each session is verified "just-in-time" when making the connection. Access to infrastructure is temporary by default, as all users need to be authenticated, authorised, and continuously validated. No permanent keys or passwords are left behind because permanent authorisation or credentials to systems are non-existent.

Teemu Tunkelo, CEO of SSH: "It's about being able to keep your data where you want it, in your data centre or in various clouds. You don't use permanent keys or passwords, and you don't rotate them, making the system resilient and less complicated." He continues: "You always know where your vital data and systems are, who has access to them, and where your critical credentials are. If needed, you can wrap your connections inside an ironclad quantum-safe tunnel to make them future-proof and virtually impenetrable."

Although most organisations have a long way to go before reaching a defensive cybersecurity posture, "the quantum threat" shows that even when grappling with today's security concerns, businesses can't afford to be complacent about future ones. Biden's push for "bold changes in cybersecurity" indicates that companies must be prepared. For organisations, starting to implement zero trust and quantum-safe access control for critical data and infrastructure is an essential journey to embark upon.

**Visit ssh.com/ssh-zero-trust-access-key-and-secrets-management to learn more**

SSH

INTERVIEW

# ‘It’s the thing we’ve been waiting for’

You might not expect a 360-year-old brand to thrive in the face of a digital transformation. But, for **Elinor Hull**, identity services director at the Post Office, the arrival of digital ID has been an opportunity to reshape the business around a secure *and* accessible offering

Emily Seares

With 11,500 branches nationwide, the Post Office has the single biggest retail network in the UK. It also carries out more than 10 million identity-based transactions annually.

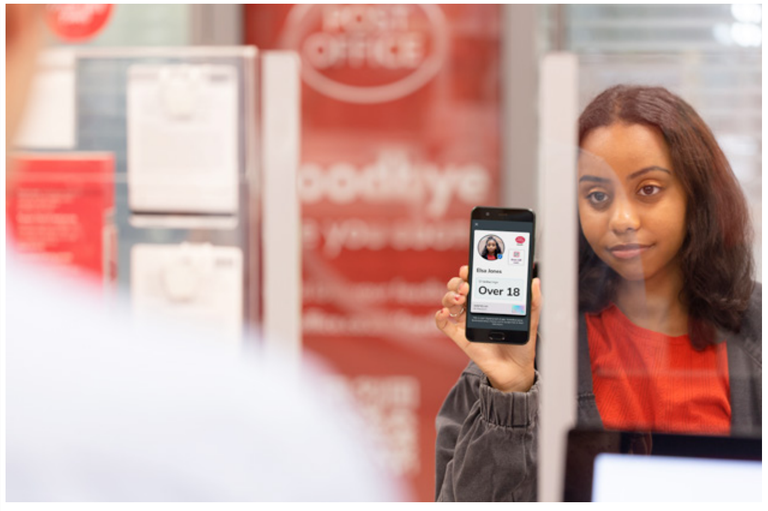
Unfortunately, those transactions aren’t all plain sailing. The volume of different identity policies in play and the many different documents required for face-to-face authentication has been a big challenge for this legacy business – made worse by an inability to seamlessly link in-person and digital transactions.

“As a portfolio business, we handle so many different transactions and a lot of services that require ID,” explains the Post Office’s identity services director, Elinor Hull.

“Whether you’re picking up a parcel, buying euros or want to withdraw cash from your bank account, you need proof of ID. And one of the hardest things our postmasters face is knowing what ID they can accept with which transaction because for many of these services we work with third parties, which have their own identity policy,” she says. Customers are also confused because they don’t understand the rationale behind the different policies.

Those are just the problems which might come up during the first stage of the transaction. Beyond establishing which ID can be used, the process of ascertaining whether the ID itself is genuine has long caused issues. “Our postmasters are not identity document experts,” says Hull. “It makes them nervous if they have to question whether a passport is genuine or they aren’t sure about a driving licence.” This can cause friction and arguments for postmasters and consumers. “That’s not what we wanted. And it isn’t how we want to service customers,” she adds.

Adapting, though, hasn’t been easy. Initial attempts to help customers access government services through Gov.UK Verify ran aground when it was confirmed earlier this year that the system would be discontinued in April 2023 after take-up was lower than expected. Even so, Hull says that the Post Office remains clear about the need to go further with integrating digital and face-to-face identity transactions. “We’ve been around for 360 years, and we definitely don’t want a Blockbuster moment,” she says. “We’re constantly looking to evolve, to ask how we can still be relevant in customers’ lives and how we can leverage the trust they’ve placed in us.”




The Post Office Pass Card provides proof of age but no other information

> **We’ve been around for 360 years, and we definitely don’t want a Blockbuster moment**

In response to these challenges, Hull launched a partnership with Yoti, an expert in digital identity and biometric authentication. This partnership has produced a free-to-use EasyID app, which Hull describes as the Post Office’s “biggest identity-related success” to date. The app combines customers’ personal data and biometrics to create a secure, reusable ID on their phone. That’s in addition to in-branch services for those customers who do not have access to a smartphone or who prefer face-to-face contact when confirming their identity.

Naturally, security has been a priority. Customers using the app can simply hold their phone up to the postmaster to show the single piece of identity information relevant to that transaction, in bold and backlit, with a recent photo to accompany it. And to safeguard privacy, identity attributes are all stored separately, with only the individual having the key and the ability to link all these pieces of information.

> **We’re constantly looking to evolve, to ask how we can still be relevant in customers’ lives and how we can leverage the trust they’ve placed in us**

“A product like this helps reinvent and refresh the Post Office brand, showing that we’re more than just bricks-and-mortar,” Hull explains.

The app also demonstrates the Post Office’s ongoing transformation into a digital identity service provider (IDSP). For instance, companies can now use Post Office and Yoti identity verification services for fraud detection, e-signatures and customer authentication, all done via secure biometric face-matching and Liveness Detection.

The app’s not the only change, either. The Post Office has introduced other identity services, including the Pass card, a physical photographic proof-of-age ID card, aimed at young people. “We’re removing some of the barriers,” says Hull, “starting with the ability to prove your identity, full stop, and then your ability to interact digitally.”

This year, the UK government released its updated digital identity and attributes trust framework, which defines rules, standards and governance oversight for IDSPs. The objective is to establish the basis for a digital identity that is as trusted as using passports or bank statements. And in June, the Department for Digital, Culture, Media and Sport named the Post Office and its partner Yoti as the UK’s first certified IDSP.

“It has been profound for us,” says Hull. “I guess it’s the thing we have been waiting for, for years. Ultimately, it is the gold standard. It is the sign that your product and your service can be entirely trusted. And that’s what has been lacking in accelerating UK adoption.”

Hull points out that the recruitment sector is already using the Post Office’s digital ID technology and with great success. The Post Office has also just completed a series of trials with supermarkets, testing the use of digital ID as proof of age for alcohol purchases. Her ambition now is to participate in a sweeping standardisation of digital identity. Higher adoption rates and more collaboration between industries will be the key to making that a reality.

To date, 3.5 million UK customers have downloaded digital identities via the Post Office’s partnership with Yoti. Hull says this is good – but not good enough.

“We need to be much closer to 5 or maybe 10 million to have the type of authority that will reassure businesses that customers will have a seamless transaction. And, equally, I can be an advocate of the product – stand from the rooftops and scream about it – but unless there are places where people can use it, it will just stay as smart technology, and nobody will care.”

It is partly a cultural change that Hull has in mind. “We need the same transformation in digital identity as we’ve seen in the payments sector, which has moved from cash to digital payments. I don’t even think about how I’m making a payment now. I can just double-click a smart watch and it’s all done,” she says. “We’ll have been successful when everybody stops talking about digital identity.”

**90%** of people in the UK live within a mile of a post office

**30,000** stores accept the EasyID app as a form of identification

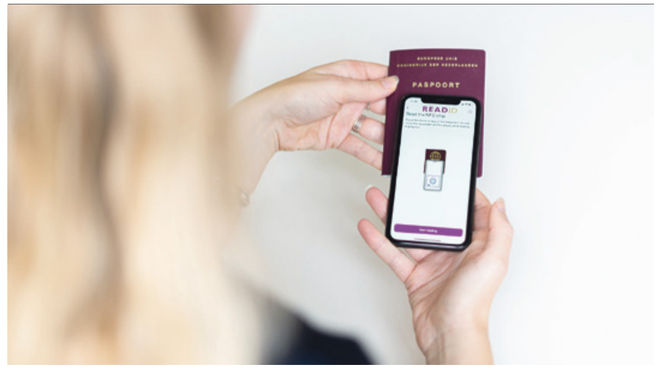
**200,000** Disclosure & Barring Service checks are processed by post offices each year

**46%** of consumers do not like it when businesses take photocopies of their ID documents

Post Office, 2021



Commercial feature




# Tackling the growing problem of identity fraud

Inverid’s ID verification solution ReadID provides comprehensive security while enhancing the user experience

Identity theft and fraud have grown exponentially over the last decade. Year-on-year, reported ID fraud cases climbed by almost one quarter (22%) in 2021, according to the UK’s National Fraud Database.

The very fact that more people than ever are working or making transactions remotely online, accelerated by the Covid-19 pandemic, means that there are also far more opportunities for criminals to attack remotely. The hackers have become more sophisticated in their methods too, so it’s critical for governments and institutions to be able to effectively and remotely verify a person’s identity.

Netherlands-based firm Inverid first developed a solution to this problem in 2015, when it collaborated with the Dutch police on an app that checks people’s identity using the officer’s smartphone. It leverages the fact that most identity documents have a very secure chip inside. Since then, it has rolled this ReadID technology out to governments, banks and other organisations worldwide.

In April 2019, the company was a key supplier for a new remote identity verification programme for the UK government’s European Union Settlement Scheme, which enables European Economic Area nationals living in Britain to apply for UK immigration status. The app, which again uses ReadID technology, can be downloaded on almost all smartphones, both iOS and Android.

It enables the user to check that the passport, ID card or residence permit is authentic, and to verify that the person in possession of the document is the same person by using biometric matching. By reading the bottom two lines on the picture page of the passport, or the bottom three lines of an ID card, known as the Machine Readable Zone (MRZ), the technology captures the required details to get access to the chip in the document using Near Field Communication (NFC).

**Authenticity proved**

After reading the data, including the original high-resolution photo of the holder, the software verifies if it’s authentic or not instantly. The data is cryptographically validated to see if it has been manipulated or if the chip has been cloned using a list of known country security certificates. Authenticity of the document can be proven with 100% certainty. This compares favourably with checking documents visually, as some fraudulent documents can hardly be detected.

If the app identifies that the document isn’t authentic – for example, if it has not been issued by a trusted source or it has been cloned – this information will be made available to the customer.

Optionally, Inverid works with partners to add liveness, presence and biometric matching through a selfie process, which matches this data against the high-resolution photo in the chip.

“Essentially, it’s an immigration e-gate in your pocket,” says Wil Janssen, co-founder and CMO of Inverid, which opened an office in London in September and has plans for another in Spain by the end of the year. “The beauty is it’s so easy to use that the customer doesn’t need to compromise on either security or user experience.”

Such is the app’s success that, by the end of June 2022, 6.7 million applications had been received through the EU Settlement Scheme (EUSS). Feedback from the 2019 EUSS survey also found that 79% of applicants said proving their identity through the app was either very or fairly easy.

The NFC technology, which meets the UK’s Good Practice Guide 45 requirements, currently works with identity documents from 163 countries. Customers can see what the data will be used for, in order to comply with the General Data Protection Regulation. No personal data is stored by Inverid.

The app’s range of uses is almost endless. As well as standard ID verification – for the likes of right to work, right to rent, security clearance, checking visas, setting up bank accounts, buying and selling property and mortgage approvals – it’s increasingly being used in remote employee onboarding and industries such as cryptocurrency, gambling and gaming, which are becoming highly regulated and where age checks or identity verification are required.

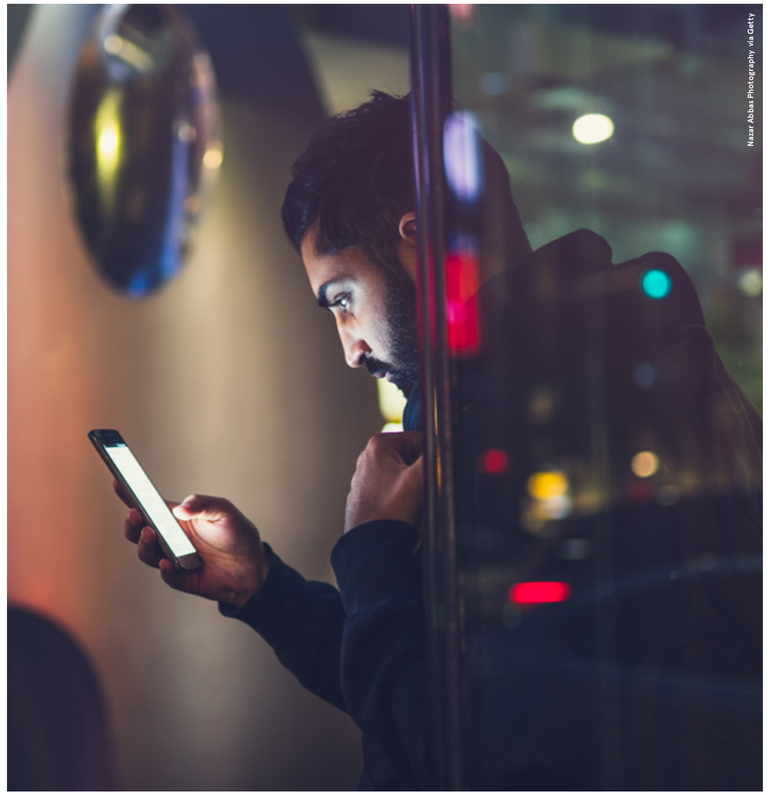
**22%**

**Reported ID fraud cases climbed by almost one quarter in 2021**

Cifas, 2022

**Learn more about trusted identity verification at inverid.com**

inverid
Creators of ReadID



Nazar Abbas Photography via Getty

MARKETING

# Incognito tracking

With the end of third-party cookies in sight, how will marketers manage the challenges of building customer profiles?

Emily Seares

Great customer experience is built around data. And the more data a company can get about their potential buyer, the more tailored that experience can be.

But the phasing out of third-party cookies will make this harder for businesses, particularly to target specific audience groups, track conversions and measure effectiveness. It means building strong first- and zero-party data has never been more important if businesses still want to compile a well-rounded picture of a customer's online identity.

According to research by cloud-based digital experience specialist Acquia, 84% of marketers say that changes to browser cookies have increased the importance of first-party data. As many as 88% feel that gathering first-party data about customers is now more important than it was two years ago.

But 73% of users browse anonymously, with just 27% choosing to log into sites and apps, according to data from customer engagement platform Braze, which analysed the behaviour of 2.5 billion active users of more than 100 popular retail and ecommerce apps for the year to October. That poses a significant problem for marketers trying to build a detailed profile of their customers and what makes them tick.

So, how are businesses tackling the issue of browsing anonymity within first-party data, and what can they do to tie the data they do gather to known individuals?

"The biggest tool in businesses' armoury is the value exchange and making that value exchange better for the customer," says Athar Naser, global director at marketing transformation consultancy CvE, which counts Vodafone, Boots and Nokia among its clients.

"Sometimes this value exchange can be product- or service-based, and sometimes it can be experience-based," he explains. "Loyalty cards or loyalty schemes are one of the biggest tactics they can use to try and convince people who aren't logged in, to log in."

Belinda Finch is CIO at Three UK and is working to do just that. The telecoms giant launched a loyalty platform for consumers in the past year and recently extended it to Three's business users. Finch says the focus has, so far, been to drive new registrations and conversions. "We are now collecting additional behavioural data that we can use. And we're considering extending this to target website visitors beyond our customer base."

> **Educating customers about the benefits of data collection could help to encourage them to part with their data**

But, pulling off an effective loyalty programme can be easier said than done. According to McKinsey's *Next in Loyalty* study, two-thirds of established loyalty programmes fail to deliver extra value for consumers. Many such schemes even erode that sense of value, the research shows.

To avoid such problems, companies should "carefully evaluate" how they are holding up their end of the value exchange bargain. So says Rose Keen, a senior analyst at marketing insights firm Econsultancy. "Personalised experiences can bring the value in that exchange," she explains. "We can see with Ikea's customer data promise, for instance, that it is improving the customer experience by personalising it from the data it collects on them. And Ikea is explicit about giving the customer control of that data," she says.

Sarah Green, marketing manager for Ikea UK, says: "Using zero-party data strengthens the relationship between us and our customers, as we can personalise experiences based on the preferences detailed directly by them. We build trust in the handling of this data by making sure we're transparent in how we use it, and only using it to improve customer experiences."

Green says these improvements then incentivise the customer to hand over more data about their preferences and interests, which helps Ikea get to know its customers even better. "We also aim to ensure that the customer feels in control, by giving them the ability to choose a preferred store and update personal details or marketing preferences through online account management at any time," Green adds.

Some industries, such as publishing, have started to look at gated content to encourage users to log in, says Shorful Islam, chief data scientist at experience-focused marketing agency Tribal Worldwide London. Meanwhile, the likes of automotive and electronics manufacturers are looking to provide additional value through reminders, information on their products and services, dashboards and reports if a user creates an account.

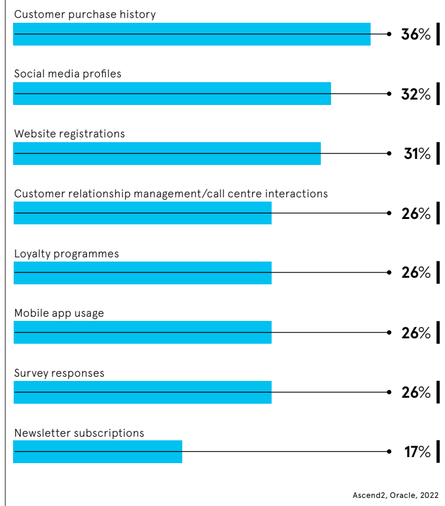
But no matter how a business decides to incentivise consumers to part with their data, this must go hand in hand with reassuring them about security, privacy and the use of this data.

"Our most recent research tells us that online shoppers care deeply about their privacy," says Claire Norburn, ads privacy lead at Google. "Shoppers who consciously agree to share their data receive the ads presented to them in a more positive light, whereas the negative impact of a poor privacy experience is almost as damaging to user trust as data theft," she warns.

Dealing with anonymity in first-party data is a challenge that won't be solved overnight. But as third-party cookies are phased out and online privacy laws tighten, offering a personalised value exchange that incentivises the provision of zero-party data, educating customers about the benefits of data collection for their experience, and being transparent about the practical use cases could all help to encourage consumers to part with their precious data.

**BREAKING THE COOKIES HABIT**

Marketers' responses to the question: "Which first-party data sources will become most valuable to address the loss of third-party cookies?"




Ascend2, Oracle, 2022



Commercial feature

# Why a digital wallet could be a friction-free pass to secure verification

The world is forging ahead with digital ID wallets while Brits are still fumbling with their cards and queueing up. Can the UK afford to be left behind when the world goes fully digital?


One company is already busy filling Britain's wallets – sadly not with cash, but with everything else a citizen might need to run their life. "Inside your wallet we are trusted to make your passport, driving licence and quite probably your bank card and your SIM card too," says Justin Walker, vice-president for digital transformation at Thales.

But unlike a physical wallet which can be lost or stolen, Thales' digital ID wallet keeps all your official documents under lock and key, helping prevent identity theft, which costs the UK nearly £4bn each year, and accelerating users through customs and banking checks.

The EU is already racing ahead in this regard. Starting with a pilot programme in 2023, every member state must offer citizens a digital ID wallet which can be used throughout the bloc. Ursula von der Leyen, president of the European Commission, says: "We have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. One that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how."

**2 out of 3**

of Europeans citizens are looking forward to the arrival of an EU-backed Digital ID Wallet for storing their ID card, driving licence and other official documents on a smartphone

Thales, 2022

A survey by Thales shows that two out of three Europeans citizens are looking forward to the arrival of an EU-backed digital ID wallet for storing their ID card, driving licence and other official documents on their smartphones. The results also reveal that 45% are relying on insecure, unofficial, DIY scans and photos of their cards and documents to help prove their identity and entitlements.

If Britain doesn't keep pace, we will be left behind, says Walker. "We are living in a global world. The real truth is that banking, driving licences and passports will eventually all be digital, and you will only use a physical passport or bank card for countries which have not caught up yet with this technology. You will need a secure platform to issue those digital credentials, securely provision them and store them into a digital wallet to keep those items safe. If we don't lead the way in the UK, the rest of the world will create the rules and we will have to abide by them."

**Time to catch up**

Whether we know it or not, our personal information is already being held in a digital wallet. Thales already provides security for 80% of the world's banking transactions and covers 19 out of the world's top 20 banks. Each has a digital safe of information on individual users to improve data security. Every time you log in, your bank can immediately see which phone, SIM card and International Mobile Equipment Identity number is being used, as well as if they have been linked to any criminal activity. And that's not all, says Walker.

"Your banking app can check up to 2,000 different parameters through Thales' software kits. If the bank suspects it is not you using the phone or entering your password, it can start ramping up the friction to stop you entering the account."

> **Inside your wallet we are trusted to make your passport, driving licence and quite probably your bank card and your SIM card too**

Now, with the acquisition of Gemalto for €4.8bn, Thales is able to allow citizens themselves to use this power safely in the form of digital wallets. A digital ID wallet will include biometrically secure personal ID such as passports, birth certificates, driving licences or Land Registry details. There is also the possibility of having more than one digital wallet, an online locked safe that relates to every area of your life. This might include a HMRC wallet – containing, for instance, instant, unimpeachable proof of tax and earnings – as well as a personal wallet with your passport, driving licence and other ID inside.

**Your data at your fingerprints**

The combination of biometrics and digital wallets can not only close criminal avenues but also speed up your life by removing red tape and daily hassles, says Walker. Travellers and lorry drivers won't have to wait and show documents in a queue. Instead, they will have a digital wallet which will show their whole ID and country of origin instantly and can even have documents sent to them while they are on the move, rather than being stamped and processed.

A digital wallet can also allow discretion. When asked for ID to enter a venue, it's possible to prove your age status without having to reveal your actual age, name or full identity. Digital wallets can also satisfy background checks without giving away all of your personal information, says Walker.

"Right now, a letting agent can ask you to submit a year's worth of bank statements for you to be a rental guarantor if one of your children is at university. It's intrusive. I wouldn't want to share a year of my bank statements – but with a digital wallet I can pass such checks without needing to have a stranger know everything about me."

**Changing the perception of digital ID**

Some may see the arrival of digital wallets as a step towards being forced by law to carry ID, or at least being pressed to produce identification more often. Former Prime Minister Boris Johnson once stated that if he had to carry a national ID card, he would "physically eat it in the presence of whatever emanation of the state has demanded that [he] produce it".

But, like many across the globe, Johnson himself has changed his mind recently, stating that digital passports are key for reducing electoral fraud. In terms of digital ID, one of the most advanced countries in the world is India, which has 95% of its almost 1 billion adults signed up to its Aadhaar system. It combines a 12 digit ID number with biometric iris scans and fingerprint data, which can be held inside a digital wallet.

When examining other countries around the world, it is clear, therefore, that different levels of progress are being made when it comes to implementing digital ID wallets. The use cases and benefits of digital ID are numerous but they cannot be realised without the right kind of support. Walker says the onus is on governments to use their pre-existing digital data more effectively. Allowing us to use it ourselves via digital wallets will also empower friction-free travel, trade and business.

"That is not related to the technology – it is related to the government. All of our future digital networks will have to connect internationally. In the future, only far-flung outposts will use physical bank cards and leather-bound passports. These nations will be left on the outside looking in."

It is essential that Britain is not one of them.

pkinnoo via iStock

LEGISLATION

# What the EU's planned law on AI means for biometrics

Artificial intelligence is advancing quickly – and Brussels is intent on curbing AI errors and overreach. Here's what businesses in the UK need to know about its proposals

Natasha Khullar Relph

The World Cup is currently under way in Qatar, and alongside the thousands of fans in the eight stadiums and on the streets of Doha are 15,000 CCTV cameras – all hooked up to facial recognition systems.

Touted by the organisers as a new standard for global sporting event security, this network of facial recognition-equipped security cameras is meant to catch any potential threats and feed them into a command-and-control centre known as Aspire. Qatar, though, is not alone in deploying this technology. Over the years, security and surveillance systems have become commonplace in soccer clubs and stadiums across the world, including in Europe. As they have proliferated across the continent, so have the cases of misidentification and discrimination.

At the 2017 Champions League final in Cardiff, more than 2,000 people were wrongly identified as possible criminals. In 2019, a 20-year-old fan was banned from the Dutch club FC Den Bosch after being falsely accused of violently confronting supporters and entering restricted areas, based on data from smart cameras. An experiment by the ACLU of Massachusetts using Rekognition, a widely available facial recognition software, led to 27 professional athletes being falsely matched to individuals in a mugshot database.

As facial recognition technology, valued at $3.97bn (£3.36bn) in 2018, has become increasingly common in the everyday life of citizens – from school lunch queues to banking services – questions about privacy and misuse are increasingly being raised. Without a robust legal framework in place that can guide the use of facial recognition and other AI technologies, many worry that great harm can be perpetuated by companies and governments acting in bad faith.

"When you deploy technology to surveil a crowd, you're already violating so many principles of due process," says Iverna McGowan, the director of the Center for Democracy and Technology's (CDT) Europe office. "Normally, you would need at least a warrant or a court order to place an individual under that type of surveillance. But if you're deploying facial recognition in a crowd setting, then you are automatically violating constitutional rights in all our countries."

The European Union is working to improve matters. The proposed AI Act aims to regulate the AI sector and set a global standard for AI oversight by guaranteeing the safety and fundamental rights of individuals and businesses. The legislation, which is currently being amended by members of the European Parliament and EU countries, would have reach beyond the EU's borders in much the same way as the EU's General Data Protection Regulation (GDPR), which applies to any business or institution that serves EU customers. And as with GDPR, the penalties for violations would be substantial: up to €30m (£26m) or 6% of global revenues, whichever is higher.

The proposal divides AI use into risk categories with a regulatory structure that seeks to ban some uses of AI, such as 'dark patterns' or 'subliminal techniques' that manipulate people, while only lightly regulating 'low-risk' categories. High-risk use cases, such as the use of AI in critical infrastructure, law enforcement, migration, border patrol, employment and education, will be heavily regulated with strict rules on transparency and data quality.

Instances of unintentional AI bias, particularly in the finance, real estate and education sectors, have been particularly commonplace. There have been reports of certain groups, including women, migrants and people of colour, denied housing or having their access to credit restricted. Since AI models are based on historical data that has been provided, any bias in the data tends to show up in future decision-making. This was demonstrated in 2020 when British students, unable to take their A-level exams due to the pandemic, were awarded scores based on an algorithm. It was later revealed that the AI had been biased towards students from wealthier schools and the results had to be scrapped.

Wilson Chan is the co-founder and CEO of Permutable, a technology start-up that creates AI solutions. "If you look at the cases that the proposed legislation talks about, the focus is on the vulnerable consumer, such as where it affects decisions with children," he says. "Those use cases represent a small fraction of how AI is being used."

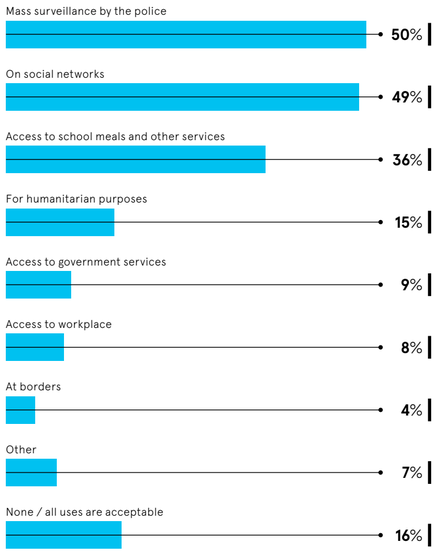
For B2B companies like Permutable, which work with corporates looking to embrace AI for the first time or to adopt it into their product line, Chan says the issue is more that they're effectively approaching clients with a black box technology.

> **Countries like Germany have pushed for tighter restrictions on facial recognition technologies, even calling for an outright ban**



**THE PUBLIC IS LUKEWARM ON THE USE OF FACIAL RECOGNITION**

Consumers' responses to the question: "In which of these areas do you think the use of facial recognition technology should be restricted?"




Biometrics Institute, 2022

"The first thing they try to do is some kind of audit around it and it's an issue for compliance departments, who ask, 'What are you actually doing, what is the product actually doing?'"

That's going to be one of the things to be addressed with the AI Act, says Chan, in that companies will have to be more conscientious about the AI used, especially if the end product is affecting someone in a vulnerable position.

One of the biggest battlegrounds around the act is biometric technology, including facial recognition. While GDPR offers some protections in this regard, it does contain exceptions, such as when the information is essential for employment, social security and social protection law. Countries like Germany have pushed for tighter restrictions on facial recognition technologies, even calling for an outright ban, but many European capitals worry that outlawing the technology could impact public security and police forces' ability to keep people safe.

Most experts agree that there are positive use cases for the technology and facial recognition can make certain identification aspects easier. But the more draconian surveillance measures, such as the mass collection of the identities of people at protests or undocumented migrants, make it a no-go zone. "This is a contentious use of technology that is extremely prone to error. Targeted facial recognition and biometric surveillance, really, in public places, is a threat to human rights and dignity that has to be prohibited," says McGowan. "Obviously, there are some stakeholders on the other side of this debate – whether that's in law enforcement or companies that profit from deploying these types of technologies – that would prefer these types of technology not to be prohibited. That's where some of the most heated debates are at the moment."

While the legislation is finalised – and the details won't become available until next year at the earliest – one thing is clear: the impact will not be the same on every business.

For companies where the use of AI falls under the low-risk category, compliance will be far simpler and less costly than for those that collect private user data or rely on AI-based ID tools. This could be harder than it seems. A survey by Boston Consulting Group shows that while 85% of organisations with AI solutions have defined responsible AI to shape product development, only 20% of organisations have fully implemented these principles.

Businesses with high-risk AI systems will, in coming years, face a legal requirement to meet a defined list of criteria before operating in the EU single market. Transparency and ethical compliance frameworks will be the key to success.

"It will hopefully make companies like ours act smarter with the data and use less of it," says Chan. "Can we lift the hood on the black box and show clients what it's doing and how it's working? That's what we're trying to address."

PUBLIC SERVICES

# The great Holyrood sign-up

What will Scotland's new digital identity service look like? And how can it avoid the mistakes of other similar schemes?

Christine Horton

The Scottish government's digital identity service will go live in 2023. Its goal is to make it easier for people to prove who they are, and that they are eligible for online public services.

The programme will be based on providing users with a single account across all public services, so they only need to provide their information once. The service is part of the Scottish government's digital strategy to build a suite of common platforms across the public sector.

"The goal is to maintain high levels of privacy and security while simplifying access to services and reducing repetitive processes for users; for example, not asking people to provide personal information multiple times in a process that has been verified elsewhere, such as proof of age or disability," says Jessica McEvoy, principal at software developer Scott Logic, which is supporting the project.

Scotland is one of many governments rolling out digital identity services for its citizens worldwide. But many hope it has learned from the mistakes of some others that have gone before it – in particular, the UK's ill-fated Gov.UK Verify scheme.

Its deployment across government was not deemed a success and didn't provide the degree of flexibility needed for many services. The Government Digital Service (GDS) admitted that: "For users, this confusing and frustrating picture of government is expensive and opens the door to fraud and error."

David Mann is managing director at dxw, an agency that develops services for the public sector. Services like these, he says, are complex and without careful consideration, technical or product-related decisions could make them inaccessible to sizeable groups of people. "This was one of the lessons learnt by Gov.UK Verify, which imposed too high a bar for some users," he explains.

So what can Scotland learn from UK government's experience?

"It's vital that research and insight are integrated into the development of the service," says Mann. "The only way to achieve this is by working in multidisciplinary teams that bring together a variety of experience and skills, rather than as a traditional IT programme. This is how you create services that are inclusive, can be sustained and continuously improved over the long term."

For its part, the Scottish government seems to have adopted this approach. It has also looked at other offerings, designing the programme to take advantage of the move towards an attribute-focused service.

To date, it has been working on the core of its offering – the components of secure sign-on and ID verification.

georgeclerkvia iStock

> **Without careful consideration, technical or product-related decisions could make the service inaccessible to many people**

Secure sign-on enables users to have just one account to securely sign in to a variety of services. Users will create an account using an email address and password, with access secured through two-factor authentication using codes sent as text messages. The Scottish government says it plans to add other ways to authenticate access to accounts, such as using telephone landlines, in 2023.

ID verification, meanwhile, is for when a public service needs to confirm identity or other personal information. Scotland's first version does this using a photo facial match against a passport, driving licence or biometric residence card.

Experian will provide identity verification services to check for evidence that the user exists, identify potentially fraudulent activity, check the validity of the documents, and match a user against the photo in the official document.

Next year will come the addition of the attribute locker. This is the function where people can choose to save their personal information to use again when applying for other public services. The first version of the locker, or store, will give people the option to reuse their verified identity. The Scottish government will then look at expanding the functionality to other types of verified information. Possible attributes could include evidence of being care-experienced, qualifications achieved or the ability to act on behalf of another person.

Digital identity vendor Avoco is helping to assess technology options for the attribute store component of the service. The firm's head of R&D, Susan Morrow, believes the Scottish government faces the same challenge that all governments have: providing a service that covers a wide demographic of users.

"This includes provisioning services that cover non-digital natives, disabled users or those with a light online footprint. The Scottish government, however, is aware of this and ensuring that the service will not be wallet-only, unlike many other services today that are only usable if the user has a mobile wallet," she says.

Indeed, Trudy Nicolson, programme director for the Scottish government's digital identity programme, explained in a recent blog that the service should be "as inclusive as possible and understand that some people may not have or want to use a driving licence or passport to verify their identity."

To this end, it is working with Experian to provide knowledge-based identity verification. This is where it asks users to answer questions about themselves, which only they would be able to answer, for instance, who their mobile phone contract is with.

Scotland says it is on track with the roll-out of its service. It has launched a production environment for the service and the current version is in use by Disclosure Scotland, which provides criminal record information to employers.

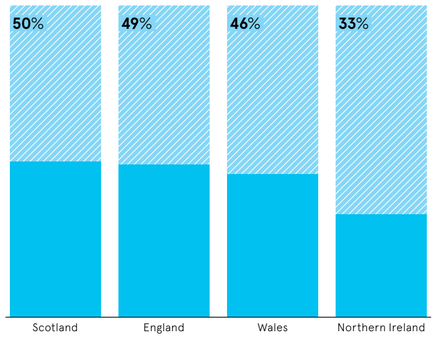
In the coming year, the Scottish government will look to add more ways for people to verify their identity, for example, through using other photo-based identity documents. It is also looking at knowledge-based verification by asking questions based on data already held within government; reuse of an identity check completed elsewhere; or the ability for a trusted person to verify someone's identity through an offline route.

Says Nicolson: "We will give people greater choice and control in the way they access public services with the aim of building a service that does not exclude people."

It's a bold claim, but if the Scottish government can learn from the mistakes of the past, it could create a model for effective national ID services going forward.

**SCOTS ARE MOST LIKELY TO USE PUBLIC SERVICES ONLINE**

Percentage of UK consumers responding positively to the question: "Do you use the internet at home to access government websites?"



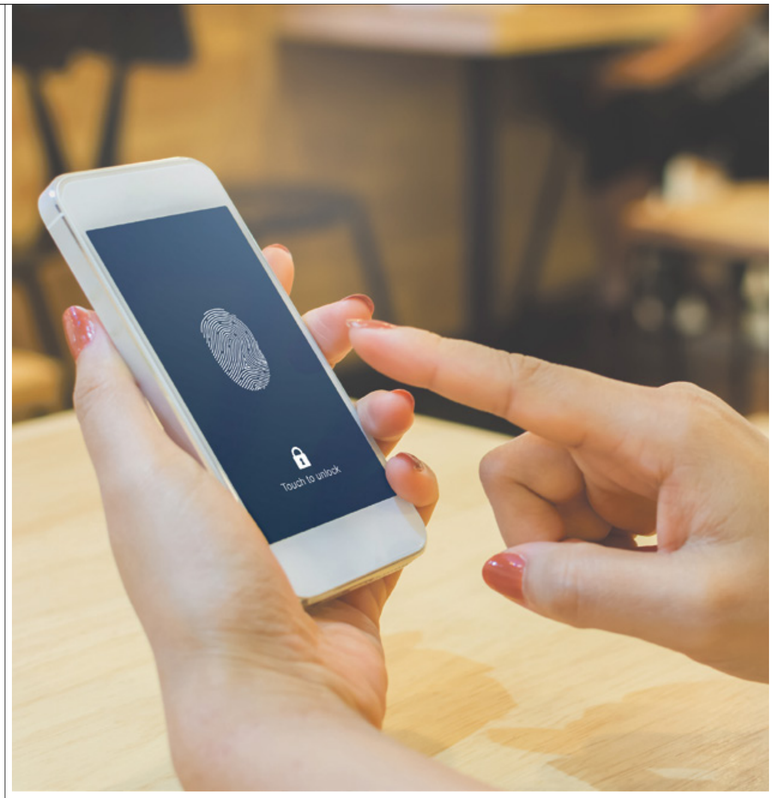

Ofcom, 2021



Commercial feature

# Banking on digital ID to reimagine the customer journey

In the Web 3.0 world, financial services have no choice but to adopt secure end-to-end continuous identity verification and authentication. But where does supercharging security leave user experience?




More than a quarter of all malicious cyber attacks are directed at banks and financial organisations. The industry is under constant attack, and the barrage is showing no sign of easing off.

Along with efforts to protect itself from increasingly prolific bad actors, the financial services industry is just that – a service industry. Moreso than most, it is starting to feel the squeeze when it comes to exceeding customer expectations for faster, simpler and more secure digital services.

Today, clients expect to arrange a car loan through their phone, download bank statements on the web and complete their daily banking transactions fuss-free. With expanding digital opportunities comes the need for greater digital precautions, and this obstacle is anticipated to become more pronounced as the industry edges closer to realising Web 3.0.

Matthew Moynahan, president and CEO of digital agreements security company OneSpan explains: "Financial organisations need to rethink their prevention strategies to safeguard customers without burdening them with more security." The parameters are changing and security will need to be all-encompassing in digital environments. "Security has traditionally focused on protecting the company's laptops, networks or payload. But now we have to look at the customer as the enterprise attack surface and how we protect every step of that customer journey," he says.

Moynahan predicts that banks will soon be dealing with millions more consumers through digital services. However, the pandemic has given rise to a new breed of customer that is reluctant to access financial services on-premise, instead opting for digital access. "We are seeing lots of trends and factors come together to drive digital service consumption – Covid-19, increased automation, a desire to cut costs, and a mass movement online. That massively increases your digital attack surface," he says.

As expectations change, financial organisations need to be actively developing authentication identity verification systems that provide appropriate regulatory compliance and security at every stage of the customer journey. This means assuring the identity of non-customers making contact for the first time, right through to the point of closing an account. Each user should know that their associated data and transactions are secured appropriately. "The market is moving towards continuous identity verification and authentication. It's not good enough to prove once that the customer is who she says she is. Just because the customer is verified once doesn't mean it's necessarily them the next time given the prevalence of identity and credential theft."

As digital and virtual experiences take over, validation technologies need to evolve. "We need to validate the customer, and the customer needs to validate us because there are so many spoof and fake services around, and we can all see the impact that has," Moynahan says. He cites the example of the recruitment industry, which faces an increasing threat from false candidates applying for remote roles through a digital side door.

Similarly, if someone applies to extend their mortgage and speaks to an advisor virtually, how can both parties be sure they're speaking with the right person?

While post-Covid consumers might prefer digital to in-person experiences, the nature of service industries dictates that when things go wrong, customers still expect a person to be available on demand. For businesses selling high-value products like mortgages or cars, the assumption is that customer satisfaction will be embedded in the process. Finding ways to add a human into the loop, securely but virtually, is essential to meeting customer demands when problems strike.

"I believe we're going to see this notion of integrating security throughout all stages using digital ID verification and authentication, not only in the physical and digital worlds but potentially also in the metaverse," says Moynahan. "Introducing people into virtual encounters is perhaps one of the biggest challenges around authentication when no one looks the same."

These security checks must be carefully designed to create a seamless user experience, while also meeting regulatory and compliance requirements. "We've all had that experience of logging into one system to make a transaction, then when you have to log in again or provide another set of identity data, we drop off the transaction because it's too much hassle," says Moynahan.

> **Security has traditionally focused on protecting the company's laptops, networks or payload. But now we have to look at the customer as the enterprise attack surface**

Ultimately, delivering the coherent, personalised user experiences that Web 3.0 enables will take industry-wide collaboration involving financial organisations and governments. "Historically, companies have competed for profit and revenue, but I hope we will see significantly more cooperation in future between entities," says Moynahan. With digital wallets, payments and identity, there is greater opportunity for sharing across a broad set of initiatives in financial services. In turn, user experience can be optimised. Banks are also in a position to profit from integrating customer journeys across platforms but will take a level of cooperation that has yet to be seen.

By adopting user-centric authentication and e-signature technologies, banks have the potential to transform the user experience. Today, when a customer makes a transaction with their bank, their identity is attached to that specific bank. If the customer then wants to make another transaction with a separate institution, there are new hurdles to overcome to prove their identity again.

Moynahan believes that banking could become an almost invisible fabric over which multiple services run, using a single, continuously authenticated identity with the right cooperation. "Just because my mortgage is with Bank of America and my checking account is somewhere else, why can't I have a single great experience across financial services?" he says. "I think the banks should leverage their trust and act as a fabric for the user experience and the identity of the end user rather than existing as islands."

This more connected banking ecosystem is poised to go beyond delivering enhanced user experiences. Banks would also benefit because this type of authentication makes compliance more achievable and has the potential to reduce operating costs.

As financial organisations turn their attention away from internal threats to protecting and authenticating digital services for customers, approaches to technology are in need of appraisal. Customers have become the attack surface in this Web 3.0 world, where previously employees posed the greatest enterprise risk. Delivering truly compelling user experiences starts without sacrificing security and is the seminal challenge in our new world.

# TAKE ONLINE TRUST TO THE NEXT LEVEL

- Identity Proofing
- Online Fraud Prevention
- AML and eKYC Compliance

jumio | KYX Platform

jumio.com/kyx