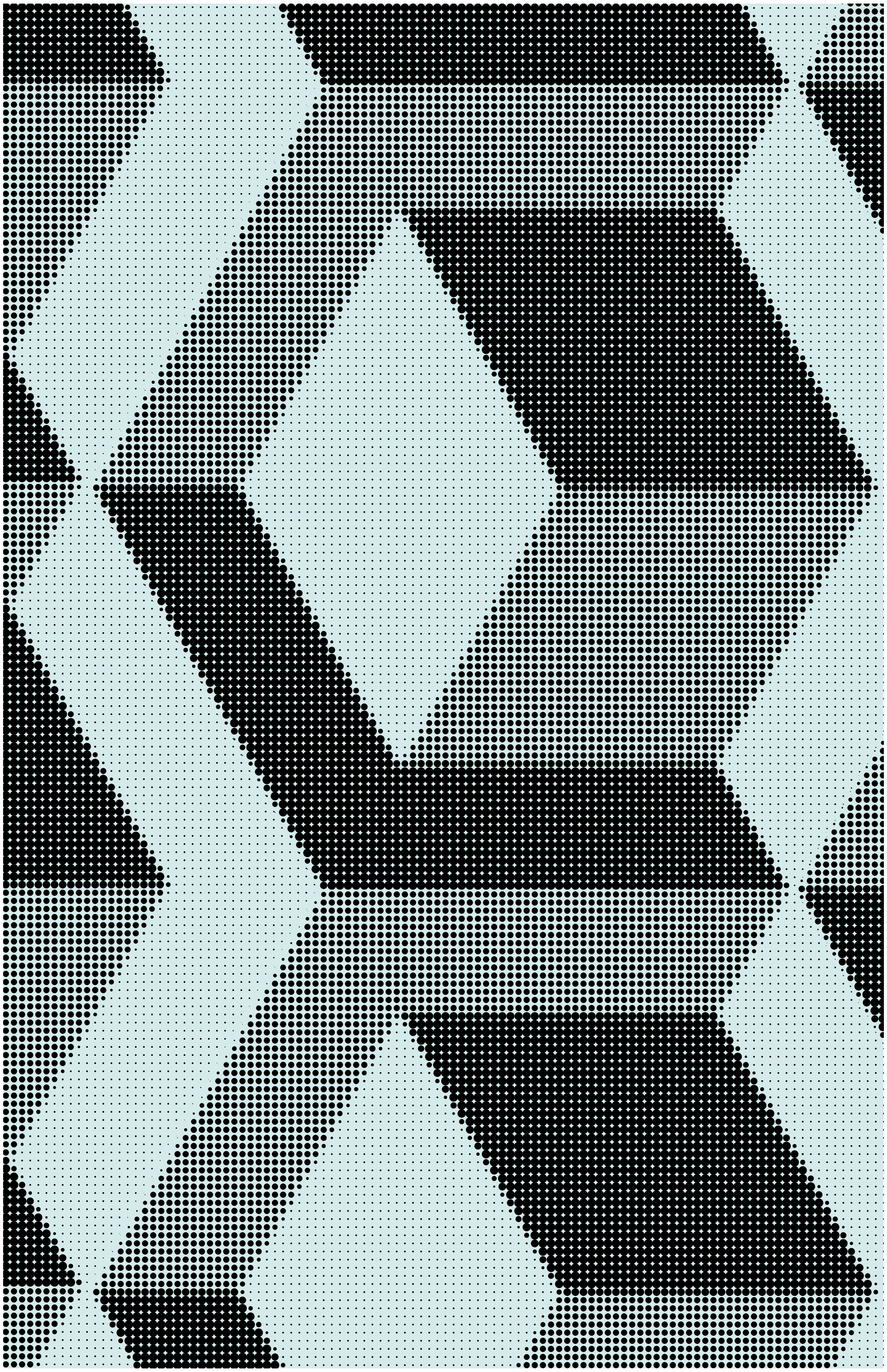
Whitepaper

January 2022

Identity: The Digital Trust Accelerator



EMEA Headquarters
20 Farringdon Road
London EC1M 3HE, UK
info_emea@okta.com
+44 203 389 8779

okta

Contents

Introduction

Over the past two years, the pandemic fueled global economic uncertainty and forced organisations to rely on digital channels to interact with customers. With the limitations on in-person contact, many had no choice but to invest in providing better digital experiences.

Today, digital services are playing an amplified role in our lives, and consumers and citizens are being asked to share more personal data. We see this as governments promote the adoption of digital vaccine passports and we see it in financial services as digital-first challengers make online the default option for banking. Both of these undertakings demand that people trust institutions with high-value identifying information.

Our research reveals that people are increasingly comfortable interacting with businesses and governments online, but they're also demanding reliable, secure and highly convenient digital experiences. People are more willing to share their data with organisations that they trust, but they're also more aware of that data's worth. This means that whenever they share their personal information, they expect to receive something of value in return. It also means that security and ease of use are absolutely essential.

Those organisations best able to deliver trustworthy digital experiences stand to win the trust and loyalty of tomorrow's citizens and consumers. To do so, they'll need to build the right technology foundation. Modernising identity management will enable users to access resources quickly and efficiently while also incorporating next-generation security controls. In the past, accessibility and security were sometimes seen as mutually exclusive concepts. Modern digital businesses must deliver both.

Above all else, our survey shows that giving away personal data is an act of trust. In return, people expect organisations to keep it safe and provide them with experiences that will simplify and enrich their lives.

Methodology

Okta engaged the research firm Statista to conduct this survey online between 12 and 27 October 2021 on behalf of Okta. The survey asked 12,010 consumers from the UK, Ireland, Germany, France, the Netherlands, Spain, Sweden, Italy and Switzerland about their trust in digital services, including those delivered by governments, retailers, banks and healthcare organisations.

Experience is all-important

A widespread shift to remote working took place in 2020, but we also saw a dramatic acceleration in consumer adoption of digital platforms and technologies. In most consumer-facing industries, offering digital experiences was the only way to continue to serve customers – and stay in business – during pandemic-related closures. As a result, people in all demographics have become more comfortable purchasing goods and consuming services online. Digital channels are now ubiquitous, and, increasingly, even the default, for everything from seeing a doctor to opening a bank account.

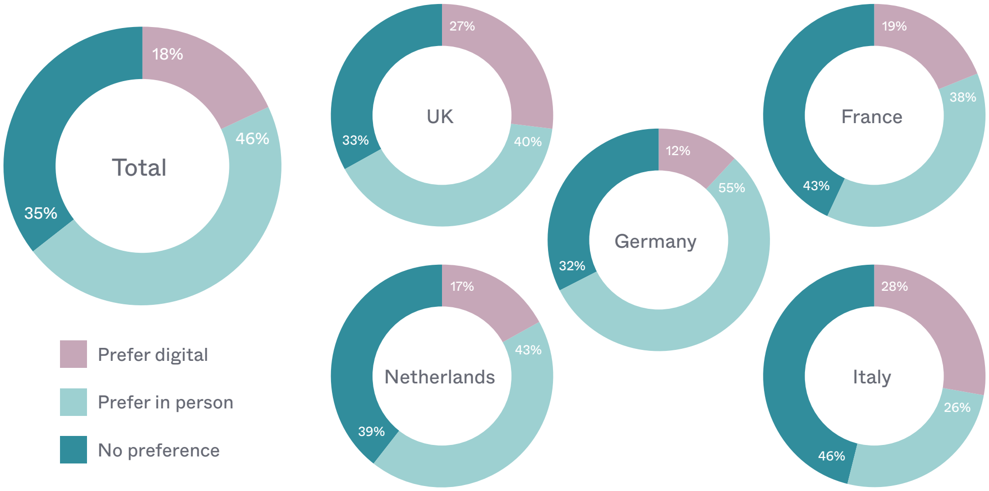
This means that consumers have a wider basis of comparison for assessing the quality and convenience of online service offerings. Our overall expectations have risen and organisations must work harder to meet them.

Digital overtakes physical for certain essential services

Consumers are increasingly willing to access services via online portals, but are less eager to embrace digital interactions when in-person experiences are perceived as more enjoyable or higher in quality. For example, as high-street banks and post office branches disappear, digital has become the preferred channel for banking and conducting financial transactions (52% prefer digital, while 20% prefer in-person) and receiving government services (43% versus 23%).

However, the in-person experience is still favored in other areas: 65% of respondents prefer in-person doctors' appointments, while nearly half (46%) prefer shopping in physical stores. Though worldwide retail e-commerce sales have seen enormous growth since the start of the pandemic, with a projected increase of more than $1.5 billion USD from 2019 to the end of 2021 (a greater-than 45% growth rate), according to research by **Statista**, many shoppers still enjoy seeing, touching and comparing merchandise in brick-and-mortar retail locations. These components of the in-store shopping experience are difficult if not impossible to replicate online.

Do you prefer shopping digitally or in person?



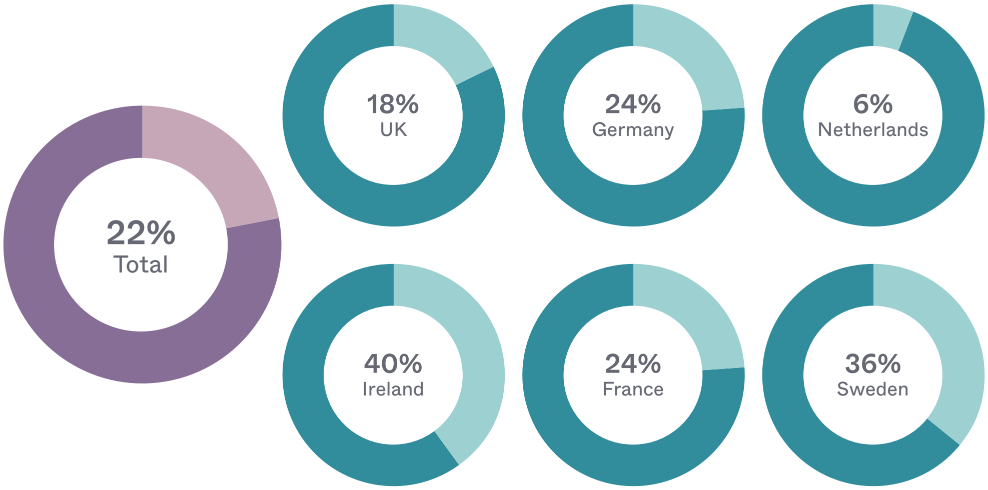
Significant national and regional differences are apparent among the survey respondents. Consumers in Italy, for example, are far more likely to prefer online shopping (28%) than the overall average (18%), while most Germans would rather shop in physical stores (55% of German respondents prefer in-person shopping). However, German consumers are more likely to embrace digital healthcare. 61% prefer to attend doctors' appointments in person (as compared to an average of 65%), while 72% of Italian respondents prefer in-person doctors' appointments. These sorts of differences indicate that emotional and cultural factors continue to play a major role in determining consumer preferences for digital or physical experiences.

Even when they're convenient and trusted, digital services cannot always replace essential in-person interactions. For organisations that provide both physical and digital experiences, taking a consistent, personalised approach across channels will be key to winning customer loyalty in a hybrid future where both online and offline experiences matter.

Fintechs forge ahead

In the financial services industry, an emerging category of new market entrants is raising the bar for speed and ease in digital banking. These fintech companies are currently experiencing a dramatic increase in popularity, with more than 1 in every 5 consumers now having an account with a challenger bank. In most countries, online-only banking is particularly favored among young people. 29% of 18- to 29-year-olds in the UK now have an account at a challenger bank, while only 13% of 50- to 59-year-olds do.

Do you have an account with a challenger bank?



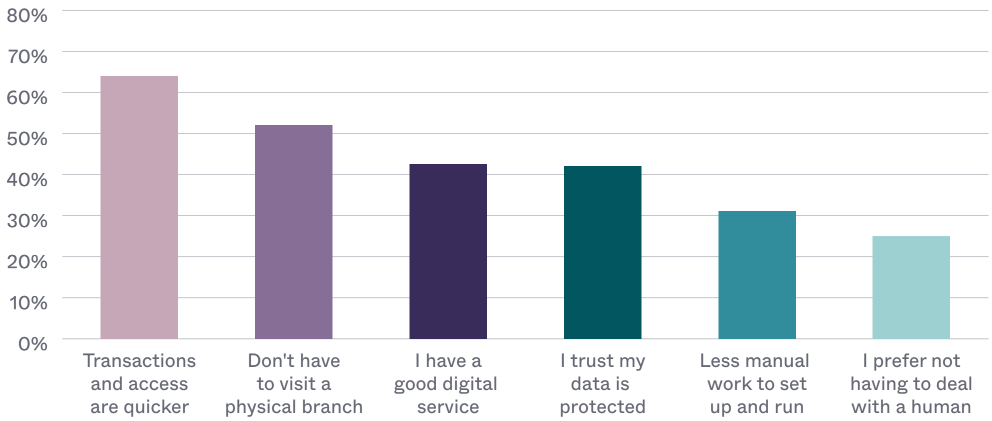
88% bank with a traditional bank in the Netherlands compared to only **47%** in Ireland

Most of us (61%) are now doing more of our banking online than we did at the start of the pandemic. And among the respondents who are interacting with banks and financial services organisations online more often than they did pre-pandemic, more than half (50.8%) are doing so because they find digital banking more convenient than in-person banking.

Consumers who are now doing more of their banking online tended to already have had greater levels of trust in digital financial services than those whose interactions with online banks have decreased in frequency or remained unchanged: 58% of those who are now banking online more than they did prior to the pandemic reported that their trust levels haven't changed over that time.

Consumers associate speed, convenience, high service quality and data protection with online banking, and these associations are what's driving increased trust in digital financial services. For instance, 64% of survey respondents whose trust in digital banking had grown said that speedy transactions and quick access to services was a primary reason for their increased confidence, while the ready availability of good digital services was cited by 43%. Nearly one-third (31%) of respondents whose trust had increased said they were more trusting because digital financial services require less manual work to set up and run.

What factors have increased your trust in digital banking?



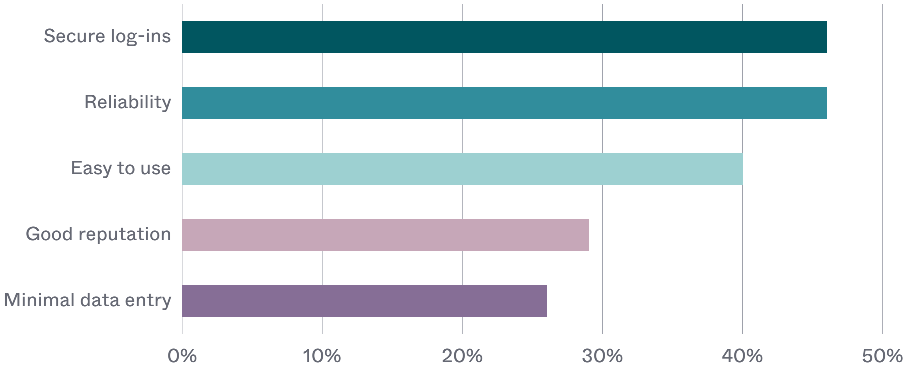
Worries about data protection and account security are prevalent among those who have lost trust in digital banking since the pandemic's start. 53% of the respondents who are now less confident of digital banking's trustworthiness say they are worried about their accounts being hacked or don't trust banks or financial services organisations to protect their data.

Even among consumers who prefer digital experiences to in-person interactions, it's relatively easy to damage trust. Weak security processes (cited by 50% of respondents), inconvenience (47%), learning of a data breach (43%) or experiencing poor customer service (37%) would all motivate respondents to switch from online to in-person interactions.

Who consumers trust is changing, as are the ways that organisations can cultivate and retain that trust. Robust data protection remains key, but making sure that online experiences are seamless and convenient is now increasingly important as well. Today's consumers are more likely to trust organisations that can deliver high-quality digital experiences, with account and resource access that's streamlined as well as secure.

Gone are the days when ease of use and security were at odds with one another. To create trustworthy digital experiences, today's organisations must deliver both – and do so consistently. Making login simple, providing top-notch experiences that are consistent across devices and incorporating security controls that introduce minimal friction – these are all ways of bringing ease of use and security together.

Top drivers of trust in online interactions



Average figure across all sectors surveyed: retail, financial services, travel, government, healthcare and utilities.

Building trust in governments and public sector organisations

As we begin to conduct more and more of our everyday life activities in the digital space, we're being asked to share personal data with a growing number of organisations and institutions, in both the public and private sectors. In a bid to rein in costs and increase efficiencies, government agencies are particularly keen to deliver services online, which requires individuals to trust them with their data.

The introduction of digital vaccine passports is a major example of how the public's confidence in government services has been under scrutiny like never before. For these systems to work, citizens must be willing to share sensitive health information with government entities. They must also trust that the digital vaccine passport issuer will have adequate security and data protection measures in place to keep their data safe.

Government services are trusted – mostly

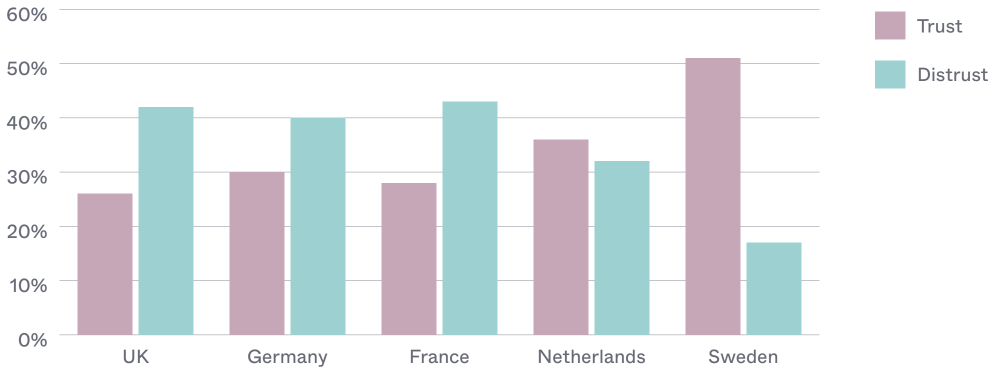
Overall, most consumers feel that they can trust the digital services provided by their government, with 41% of survey respondents stating that they trust government websites and login portals for services like filing taxes or checking on drivers' licence status, and only 31% reporting that they distrust their government's digital services.

However, there are marked disparities between countries. In the UK, France and Germany, there's slightly more distrust than trust, while in Sweden trust levels are impressively high. 56% of respondents in Sweden voiced trust in their government's digital services, while only 18% were distrustful.

There's also greater distrust among young people. Again, this is particularly true in the UK, France and Germany, with 42% of 18- to 29-year-olds in the UK expressing distrust in the digital services provided by their government, as opposed to 26% of 60- to 75-year-olds. It's imperative that governments win the trust of younger citizens, since they will become the principal users and funders of public services in the future.

Governments that fail to provide trustworthy digital services to their constituencies stand to lose a great deal. One-third of the respondents who lacked trust in the digital services provided by their government said that their distrust could lead them to consider changing who they vote for. As many as 47% of the distrustful 18- to 29-year-olds in the UK might shift political allegiance as a result of their distrust, with 42% of people in the same age group in Germany feeling similarly.

Trust in government digital services among 18-to-29-year-olds



In Sweden, digital investment pays back in trust

Sweden is a leader in digital public services[1], which may explain high levels of trust and receptiveness towards digital IDs.

56% trust government digital services vs **18%** distrust

72% of digital ID supporters say they sound easy to use vs **55%** survey average

Digital IDs coming into widespread use

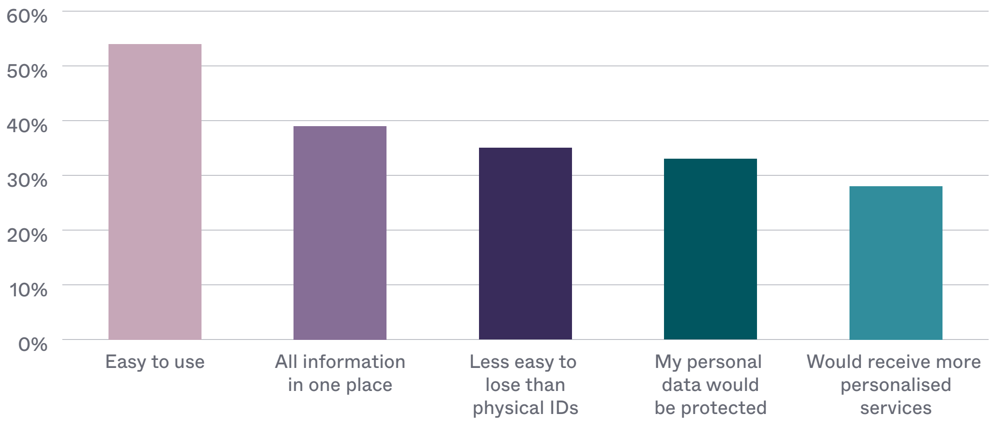
Digital identity verification systems have been the subject of public debate, but are increasingly gaining widespread acceptance. 63% of survey respondents would be comfortable having basic personal information such as name, birth date and photo incorporated into a digital ID, though only 9% would feel comfortable with the inclusion of financial details.

Those respondents who are willing to accept digital IDs are ready to do so primarily because of ease of use (55%) and convenience. 39% of respondents would prefer to have all their information in one place, and 35% believe that physical IDs are easier to lose or misplace than digital IDs.

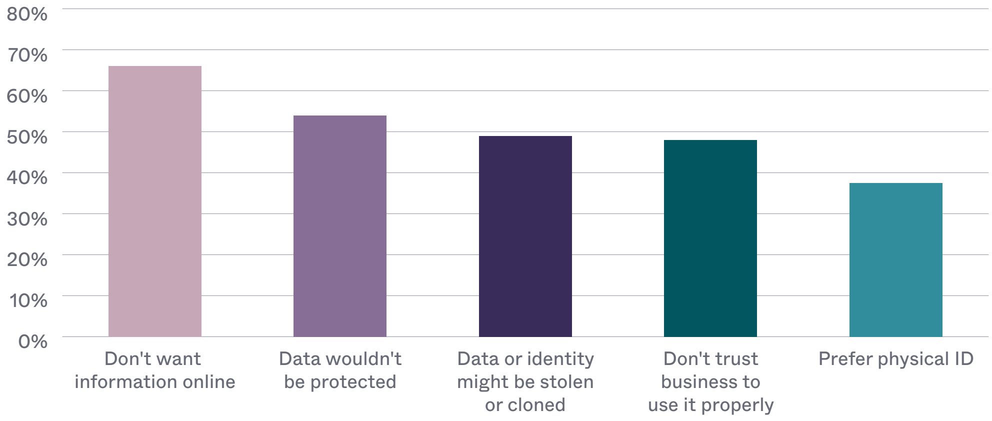
[1] Digital Public Services in the Digital Economy and Society Index

Among the respondents who do not want any form of digital identification, a dislike of having their information be available online was the grounds for opposition in the largest group (66%). 54% voiced concern that their data would not be protected, and 49% expressed fear that their data or identity might be stolen or cloned. Allaying these security concerns will be essential for governments hoping to increase public acceptance of digital identity systems.

Why would you feel comfortable with a digital ID?



Why wouldn't you feel comfortable with a digital ID?



COVID-19 vaccine passports have provided citizens around the world with a first experience of a digital ID system. Most survey respondents (55%) are supportive of government-led vaccine passport initiatives, with 66% of supporters saying that they feel safer when vaccine passport technology is in use and 50% reporting that they like having proof of their vaccination status on their devices.

Governments have invested heavily in making sure that vaccine passport systems are accessible and easy to use. These investments are already paying off in terms of widespread and growing acceptance of this technology, a phenomenon that's grounded in user trust.

66%	say vaccine passports make them feel safer
50%	like having proof of vaccination on their devices

In general, our research reveals that today's citizens are increasingly willing to share their personal data – including sensitive health information – with public sector entities if they believe that the benefits of doing so outweigh the risks. For governments and citizens alike, there are many advantages to adopting digital identity verification systems. These include speed, ease of use, cost savings, efficiency and centralised information access.

But to facilitate the adoption of digital IDs and online services, governments must continue to invest in cultivating users' trust. This means incorporating security controls that are robust and reliable, but that don't introduce unnecessary friction into the end user's login experience. Every time that friction occurs, it undermines citizens' primary reason for turning to digital platforms in the first place – convenience.

> “
>
> By 2025, 35% of organisations will replace net promoter score-like metrics with trust indices in RFPs to align traditional security and risk solutions with customer success, brand and reputation. [These indices] will be embedded into RFPs when acquiring new products and services and vetting vendors.
>
> IDC FutureScape: Worldwide Future of Trust 2022 Predictions,
> Doc # US47193621, October 2021

Private sector organisations as stewards of trust

When the General Data Protection Regulation (GDPR) first came into force in 2016, the rule strengthened individuals' right to privacy and control over their personal data. Explicitly designed to harmonise data protection laws across the entirety of the EU, the legislation regulates how private sector organisations must protect data belonging to EU citizens. The GDPR has come to be seen as a model for data protection and regulation, with similar legislation subsequently having been passed in many other countries and jurisdictions.

Within Europe and the U.K, there's widespread public awareness of the GDPR's existence and import. A clear majority (55%) of survey respondents voiced support for the legislation. And among these supporters, 76% stated that they believe that enforcing data privacy initiatives should be a key responsibility of states and governments. However, only 34% are confident that their personal data is better protected as a result of the GDPR's existence.

Since the GDPR's adoption, many citizens have become more conscious of the value of their data, the potential consequences of its theft and the importance of privacy. As a result, people increasingly view sharing their data as an act of significant trust. But many believe that the GDPR's provisions don't go far enough: an organisation that wants to earn and retain its customers' trust will need to demonstrate that there are clear benefits to sharing information with that organisation, and that the security measures in place to protect its customers' data are robust.

Willing to hand over data – but only in exchange for something that's of real value

Most survey respondents (64%) said that they'd be willing to trade their personal data for certain benefits, including medical diagnosis or treatment (40%), discounts when making a purchase (33%) or entry to a public venue such as a restaurant, bar or pub (22%). These answers reveal growing public awareness of the monetary and utilitarian value of personal data, along with an increased willingness to treat data as an exchangeable asset.

As is the case with many facets of digital trust, attitudes about when it's worthwhile to trade personal information for particular benefits vary across countries and demographics. People in the Netherlands are particularly protective of their identity information, with 4 in 5 Dutch respondents stating that they're unwilling to give up personal data for access to hospitality venues.

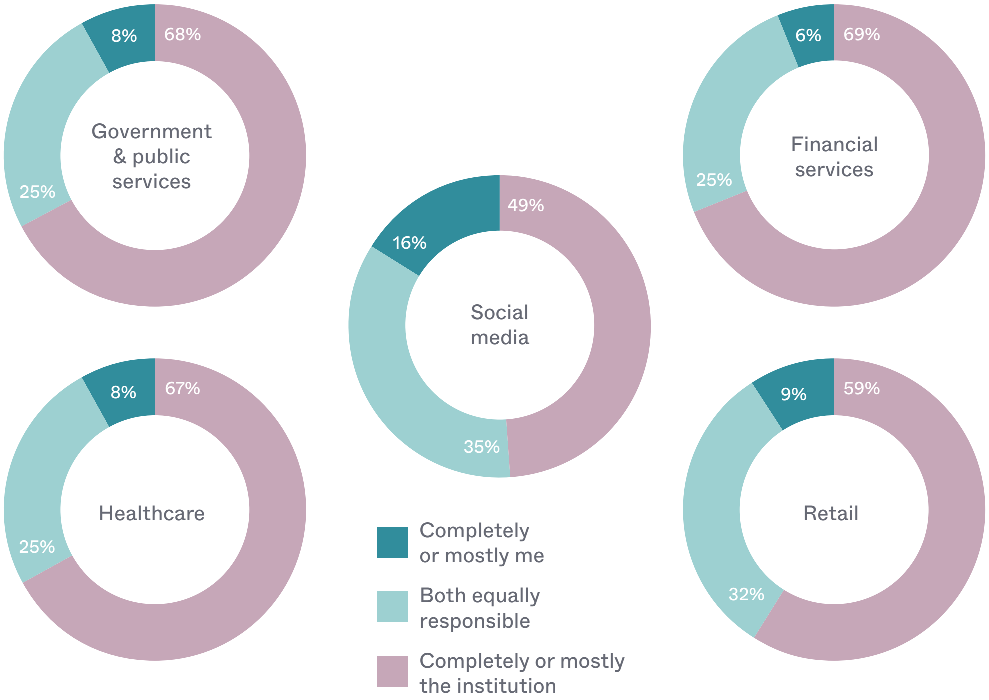
Our data is valuable

As customers and citizens, we're increasingly conscious of the worth of our data.

33%	of us would be willing to trade it for discounts on goods and services
22%	would share it to gain entry to restaurants, pubs and bars

In tandem with this greater willingness to exchange data for money, goods, services or other benefits, there's a stronger popular belief that public and private sector organisations bear primary responsibility for protecting the personal data and digital identity information that's shared with them. This was true for every type of data we asked about in our survey, but the more important the data was perceived to be, the higher the expectations were that organisations would protect it. Hence, governments, healthcare organisations and financial services firms are seen as bearing a greater burden of responsibility than social media companies.

Who's responsible for protecting your personal digital identity and data?



For the most part, today's consumers are open to sharing their data with public and private sector organisations. They're increasingly aware of the value that information exchange can bring and are willing to make tradeoffs if they believe that they will benefit. At the same time, however, the more value that they understand their data to hold, the more strongly obligated they feel companies, government entities and other organisations should be to protect it. Overall, 50% of survey respondents said they believed it was the government's responsibility to implement rules and regulations to protect their data, with rates significantly higher in certain countries such as Sweden (62%) and Spain (61%).

Just as is the case for governments, it's essential that private sector organisations invest in cultivating users' trust. Consumers increasingly believe that companies should be held responsible for protecting their customers' data. At the same time, people are more willing to share their information if they believe they'll receive value or benefits in return for doing so.

Of course, providing secure, reliable, smooth and frictionless access to online resources is of enormous value in today's digitally-enabled world. The businesses that are best able to supply their customers with these sorts of digital experiences will be first in line when it comes to earning trust.

> “
>
> Data security, confidentiality, integrity, and availability are now key issues for any organization. Even more imperative is to ethically use data and comply with a complex web of industry and regional regulations.
>
> IDC FutureScape: Worldwide Future of Trust 2022 Predictions,
> Doc # US47193621, October 2021

Conclusion

In the wake of 2020’s shift to digital, both public and private sector organisations have embraced newly-expanded opportunities to supply products and deliver essential services online. Digital platforms have become sources of revenue, but they’ve also gained currency as a means of connecting with large audiences – of citizens, healthcare consumers and members of the general public.

We’ve all become more familiar – and comfortable – with shopping online, making telehealth visits to care providers, internet banking and consuming digital government services. As our comfort and familiarity with the digital world has grown, so has our awareness of our personal data’s value.

This doesn’t mean that we’ve become unwilling to share our data. In fact, the opposite is true. Consumers may be more willing than ever to share personal information with brands and government entities, assuming that a solid foundation of trust has been established, and that they know they’re receiving real benefits in exchange for their data.

People seek out digital services primarily because of the ease and convenience that they offer. If government entities, healthcare organisations and brands want to win and retain the trust of today’s citizens and consumers, they must be able to deliver these benefits, which are in demand and widely expected. The key to doing so is delivering secure, consistent, personalised and reliable experiences to the users of their digital services – every time they log in.

Identity lies at the heart of the ability to deliver such experiences. It underpins both usability and security in today’s digital-first world. Organisations that place identity at the centre of their digital transformation strategies stand to delight their customers and earn their loyalty for the long term.

Securing trust with CIAM

Great user experiences drive trust. Here's how a secure customer identity & access management (CIAM) solution like Okta's can make the user experiences that your organisation delivers stand out from competitors'.

Focus on UX

Take users swiftly to what they want. A CIAM solution streamlines the digital experience to enable quick, simple login and minimal data input.

Build next-level security into your systems

Cultivate trust and prevent identity theft with security controls that add minimal friction, such as multi-factor authentication.

Personalise the experience

Unify your identity data to create a single source of truth for every customer, helping you deliver personalised experiences that drive loyalty and trust.

Automate GDPR compliance

Keep on top of the most recent GDPR requirements with an identity solution that automatically ensures consent is correctly requested, stored and updated.

Be consistent across devices

Create great omnichannel experiences that are consistent across all devices, platforms and even brands by tying individual profiles securely to users' unique identities.

About Okta

Identity is the foundation to build trust-based, secure organisations. With the Okta Identity Cloud, business leaders worldwide can confidently create the best digital experiences for their employees and customers. Secure your employees – wherever they are – with Okta's workforce identity solutions. Get the tools to secure and automate cloud journeys, with full support for hybrid environments along the way. Use Okta's customer identity solutions to build secure, seamless customer experiences that your developers and users will love. To learn more, visit **okta.com/uk**.