cpl.thalesgroup.com

THALES
Building a future we can all trust

2024 Digital Trust Index

Building Digital Experiences that Enhance Consumer Trust

Endorsed by

kuppingercole ANALYSTS

#2024TrustIndex

Executive Summary

Trust is not a monolithic construct. This is why it takes brands months and sometimes years to earn the trust of their customers. These customers in turn become brand advocates. First impressions certainly count, but it is a combination of multiple good interactions that lead to a sense of trust in the minds of customers. The digital realm and thereby, digital trust, are no different. This report aims to share insights from consumers around the world, to guide businesses on how to build trust with their customers.

The right balance of user experience, security and increasing data privacy tend to govern how trustworthy a brand is perceived to be. This survey reveals how this balance can be nuanced in different sectors, regions and demographics. Notable results, such as **46%** users expecting a clear view of what they've consented to, clearly demonstrate how savvy the modern digital user is.

Multi-Factor Authentication (MFA), often conceived as the enemy of a frictionless user experience, is seen as a must-have by **41%** respondents and a good-to-have by another **40%**.

Despite the proven security advantages MFA brings, some CISOs and CIOs have hesitated to integrate it into digital journeys, fearing an increase in friction — unaware that users, in fact, value and expect such measures.

How much friction is enough though, when **53%** of customers suggest that they would give up their interaction with a brand if they're hung up for more than two minutes in their interaction?

Artificial Intelligence (AI) adds another layer to the trust discussion; how do consumers, in general, feel about the use of generative AI to enhance the user experience, versus the personal data risks it embodies?

The rich feedback garnered from this survey provides valuable insights for CIOs, Chief Digital Officers, or CISOs striving to achieve the optimal balance between security, user experience, and privacy. The report concludes with a set of recommendations to help build the foundations of trust with today's consumers.

Sponsored by

EXCLUSIVE NETWORKS

> MFA is often perceived as the enemy of a frictionless user experience, yet 81% expect brands to offer MFA.

Key Takeaways

Essential services top the Digital Trust Index

The **most** trustworthy industries:

44% Banking
41% Healthcare
37% Government Services

The **least** trustworthy industries:

7% Media and Entertainment
6% Social Media
5% Logistics

(Percentage of customers who are willing to share their personal information.)

No compromise - consumers want better experiences and technology

Across all industries, consumers place high importance on both an online experience and data security.

You have to earn your customers' data

The majority **(89%)** would consent for organizations to use their data – but only if certain caveats are met. Nearly a third **(32%)** will only consent to what is necessary, with three in ten **(30%)** expecting to be able to control what data they share. As many as **87%** of consumers also expect basic levels of data privacy to be met, including the right to be informed their data is being collected **(55%)**, and the right to have that data erased **(53%)**.

You blink, you lose - customers are time conscious

Consumers want their interactions to be quick, convenient and hassle free. Over a fifth **(22%)** give up within a minute if they're having a frustrating online experience – with the likes of password resets and having to re-enter personal information topping the list of frustrations.

Contents

Key Takeaways 4

The Global Context 6

Climbing the Digital Trust Index 12

Building Loyalty through Digital Experiences 16

The Potential of Emerging Technology 21

Country and Demographic Spotlights 22

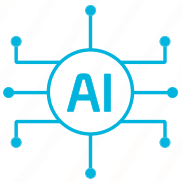
Striking the Balance 25

About the Research 27

51%

of your own people aren't happy either

Only **51%** of employees believe their employer values the importance of a good digital experience, with complex password resets and trouble accessing accounts remotely hampering productivity.



57%

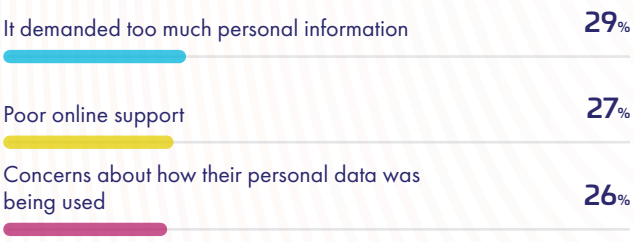
Keep AI close, but data privacy closer

Artificial intelligence (AI) was identified as the technology perceived most likely to have a positive impact on our online interactions with brands. However, fears on what it means for data privacy overshadows the optimism, with **57%** saying they feel nervous about what this will mean for their data privacy.

The Global Context

Data security and smooth digital experiences have become non-negotiables for consumers today. You can't have one without the other, and customers are prepared to abandon brands if either is lacking.

Reasons consumers have left a brand in the past 12 months



Trust and experience go hand in hand, and collecting data is no different. Four in five **(80%)** customers expect a fully digital onboarding experience, and the majority **(89%)** will only share their personal information if certain caveats are met. This creates a delicate tightrope that businesses must walk; security, privacy and experience all ultimately ladder up to trust.

80%

customers expect a fully digital onboarding experience

89%

customers will only share their personal information if certain caveats are met

Caveats for consenting to share personal information

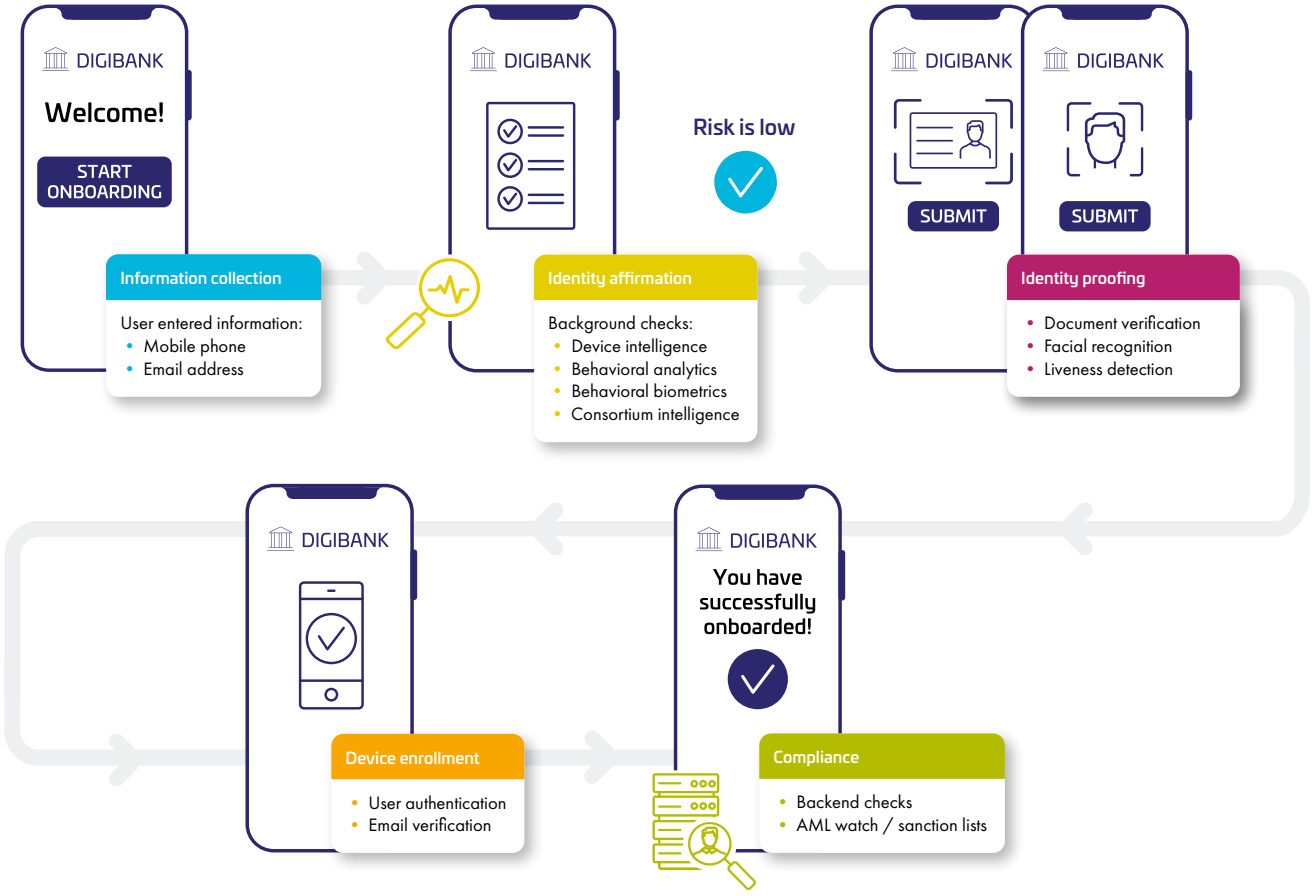
These demands dictate how trust is built. The more a customer trusts an organization, the more likely they will be to engage with them on a deeper level, thereby positively impacting the CLV (customer lifetime value). So, which sectors are currently leading the way?

> **The more customers trust an organization, the more likely they are to engage on a deeper level.**

Did you know?

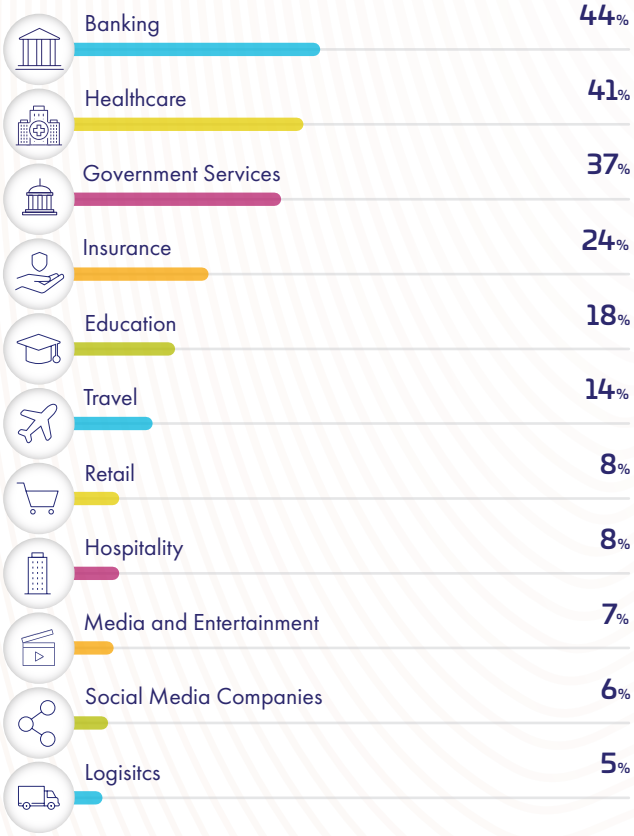
80% customers expect a digital onboarding experience, and why not!

Take the example of this new banking consumer. A conventional onboarding process would require her to visit the branch, get in a queue and wait for a long time for the bank to run its administrative processes. A digital onboarding experience still requires an excessive amount of back-end processing, but hides that complexity from the consumer who can be up and running in the matter of a few clicks.



2024 Trust Index Ranking

Customers were asked what sectors they were most comfortable to share their personal information with.



The research confirmed that consumers place more trust in banking, healthcare and government services when it comes to sharing their personal data – a universal trend we've seen across all the markets surveyed. This is perhaps unsurprising when considering how highly regulated these industries are, the types of information they are responsible for handling, and the measures they have put in place to keep consumer data secure.

For example, banking tops the trust Index, and is also subject to directives such as the Second Payment Services Directive (PDS2), in Europe, at least. This legislation was introduced not only to promote competition and innovation within financial services companies in EU, but to enhance the security of online payments. Key mandates of the legislation include the need to offer at least two of the following forms of authentication:

- Something the customer **knows** (e.g. a password or a PIN)
- Something the customer **has** (e.g. a smartphone or smart card)
- Something the customer **is** (e.g. fingerprint or facial recognition)

The Upcoming PSD3 Legislation

As an update to PSD2, PSD3 aims to even further protect consumer's rights and personal information. Intended as an amendment to the existing PSD2 framework, PSD3 addresses emerging challenges and opportunities in the digital payments landscape. It seeks to promote fair competition, advance open banking, enhance cash availability, improve consumer rights, and streamline regulation and enforcement. The directive, expected to be finalized by late 2024, allows member states two years to incorporate the standard into national legislation, with an additional two-year grace period for companies to comply, providing ample time for adaptation within the European Economic Area (EEA). Interestingly, **44%** respondents from European countries (more regulated) show trust in banks compared to **35%** in the U.S., which has a more fragmented data protection regulation.

Sectors at the bottom of the list may want to look at best practices implemented by the more trusted and regulated sectors.

The regulation also included enhanced customer protection methods, and gives them greater consent and agency over how their data is used.

While businesses are subject to international data privacy laws no matter the sector, those further down the rankings have been subjected to fewer directives directly addressing both data security and privacy. Those sectors further down the list may want to look at the best practices from these more trusted and highly regulated sectors; they equally need to build this trust in order for customers to share their data and in turn receive a better experience.

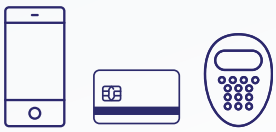
Throughout the rest of this report, we'll explore what organizations can do to tread this balance, and climb the Digital Trust Index.

Did you know?

Financial Institutions are mandated in most jurisdictions to use SCA (Strong Customer Authentication). SCA requires at least two of the following elements (or "factors") for conformance.

What I have

Device



Possession

What I know

PIN or Password

Knowledge

What I am

Physical Biometrics

Inherence

Climbing the Digital Trust Index

Most customers **(89%)** are willing to share their data with organizations, but that does come with some non-negotiable caveats. More than four in five **(87%)** expect some level of privacy rights from the companies they interact with online.

The most in-demand expectation is the right to be informed that their personal data is being collected **(55%)**. This is closely followed by the right to have their personal data erased **(53%)**. When asked about other privacy rights:

39%
expect the right to **correct their personal data**

33%
expect the right to **request a copy of their personal data**

26%
expect the right to **move data from one platform to another**

> **87% of customers expect some level of privacy rights from companies they interact with.**

These expectations extend to when a customer stops using a brand or service. A third **(32%)** stated that they would not be comfortable if that company still had access to their data – and would take action to rectify it. Just **16%** said they feel comfortable because they believe their data will be used for legitimate reasons.

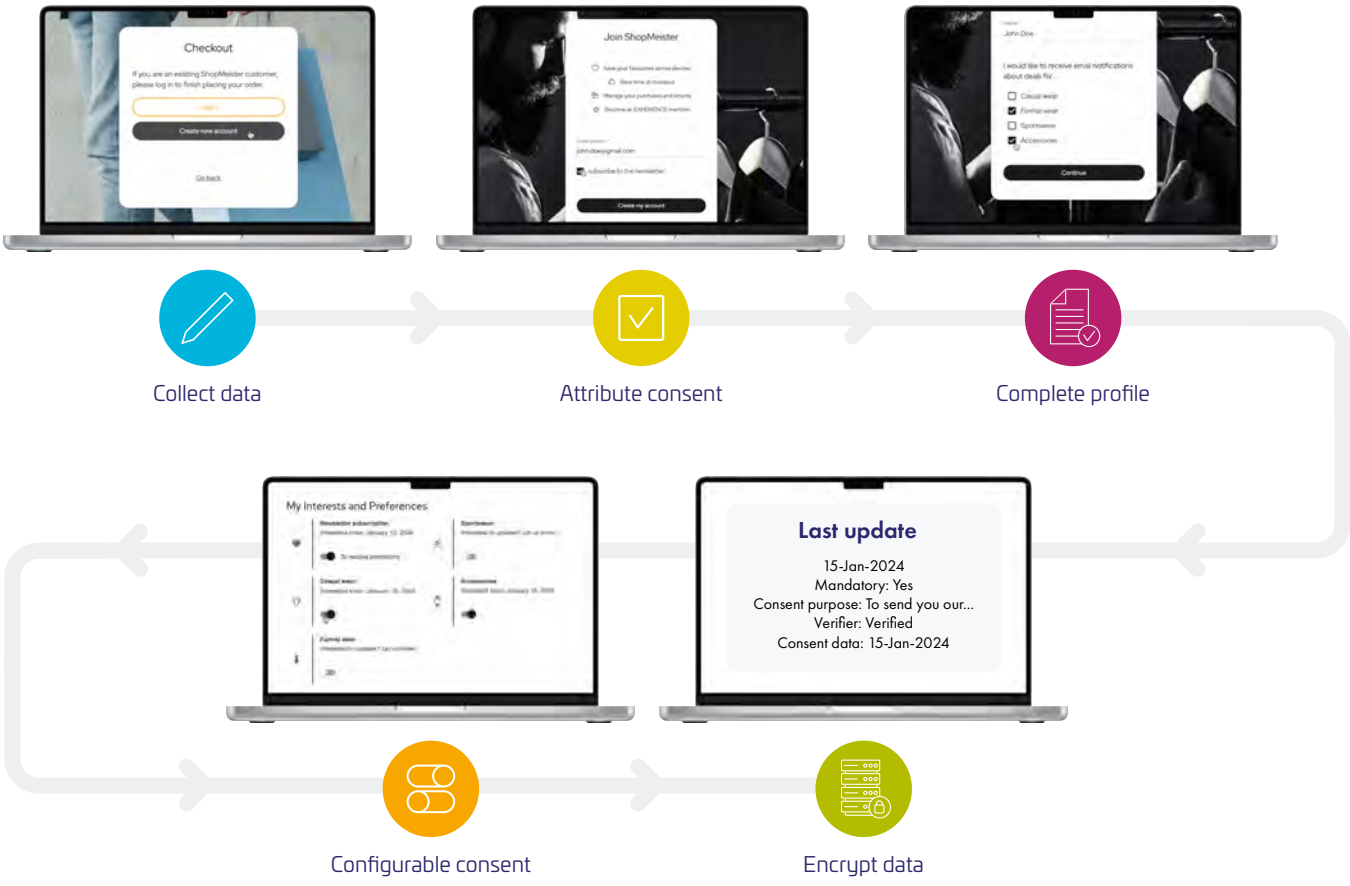
Four in five **(81%)** consumers want brands to offer two-factor authentication (2FA), so this is one means for a brand to be seen as trustworthy to their end-users. This demand highlights that customers are prepared to add some friction for that extra layer of security.

The good news is that companies can strike a balance here by using risk management technologies that run silently in the background to introduce risk-based authentication (RBA) / adaptive MFA. By implementing this, a brand can minimize friction by only asking for additional authentication when the risk is high.

Did you know?

Data Subject Requests

Data Subject Requests (DSAR, but also referred to as SRR, SAR or DSR) is an important legal entitlement for citizens to make a request about their data held by organizations. GDPR (General Data Protection Regulation) in the EU, PIPEDA (Personal Information Protection and Electronic Documents Act) in Canada and CCPA in the state of California are just a few examples of regulations that enable this provision for citizens, and making organizations liable to comply.

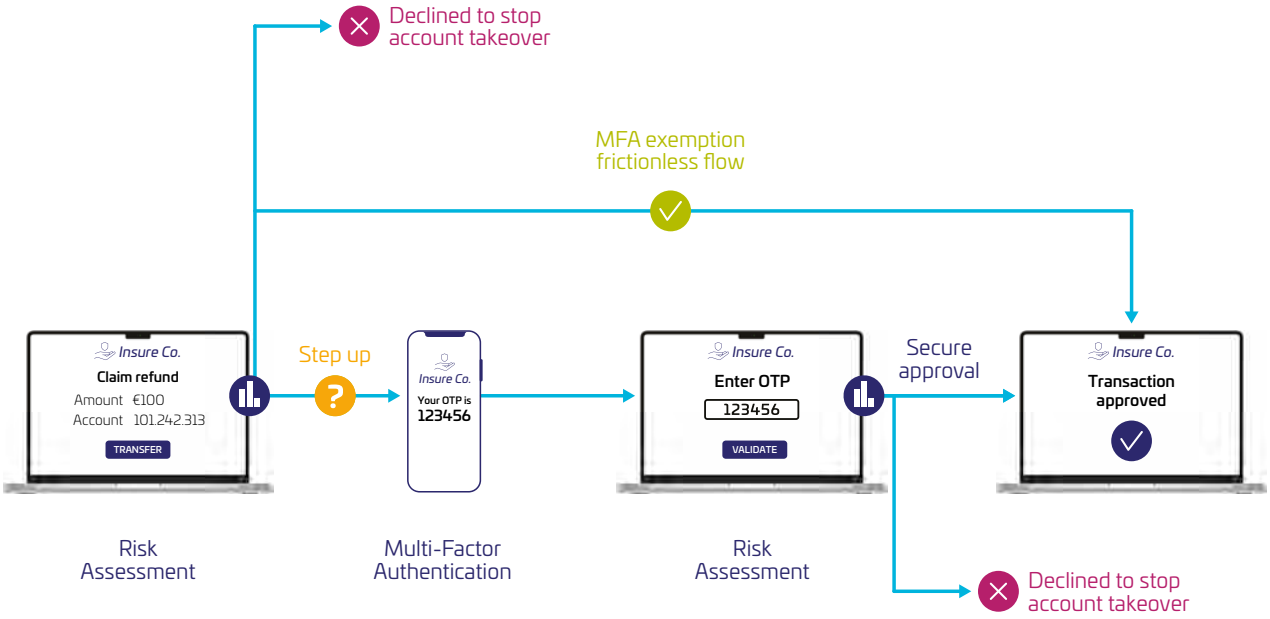


Focus on Privacy by Design – make privacy an integral part of your user journey. In order to address data subject requests, companies need to store metadata about that sensitive data.

Did you know?

Risk-Based Authentication (RBA)

Risk-Based Authentication (RBA) is a type of authentication that varies based on certain behaviours and characteristics. It automatically undertakes a risk assessment of a customer and determines threat risk based on those characteristics – including a user's IP address, physical location, browser history, device and their behaviour. RBA checks each transaction and user on a case-by-case basis, unlike traditional systems. For consumers it offers the highest level of security, with the least interruption or disruption to their day-to-day user experience.



This simple RBA example depicts how authentication can be made more frictionless and more secure. RBA runs in the background, evaluating when and if, "stepping up" to a stronger form of authentication is necessary.

Building Loyalty through Digital Experiences

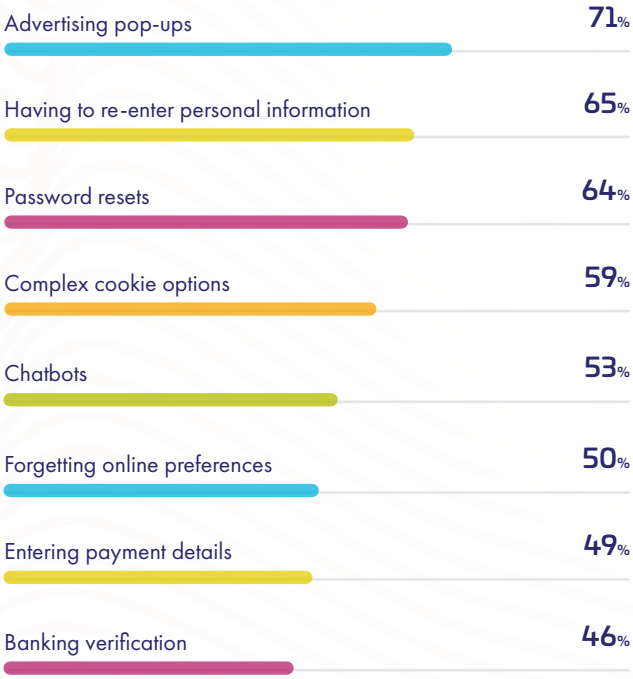
Customers value their own time greatly and want hassle-free interactions with online brands. Nearly three quarters **(72%)** want their interactions to fit in around their working day (9-5). These interactions need to be swift too – over a fifth **(22%)** will give up after a less than a minute of having a frustrating customer experience.

Is there a killer feature that can act as a silver bullet for great digital experiences? Not quite. However, having a clear view on what users have consented to share is seen as a must-have by **46%** of the respondents, with an additional **36%** feeling it's a nice-to-have. Some regional and demographic nuances also seem interesting for companies looking to micro-segment. For instance, **30%** respondents aged 45-54 and **40%** aged 55+ find chat bots for self-service as not useful. This reflects how important it is to understand the preferences of your target demographics.

The biggest source of online irritation? Advertising pop ups. These emerged as the number one online frustration among consumers **(71%)**, closely followed by password resets **(64%)** and having to re-enter personal information when they have used the brand before **(64%)**.

Over 22% will give up after less than a minute if the interaction is not hassle-free.

Biggest online frustrations



Passkeys

Passkeys, cryptographic alternatives to traditional passwords, serve as unique identifiers generated by a user's device for secure authentication. Unlike passwords, passkeys are less prone to compromise and contribute to reducing the risk of unauthorized access, phishing, and credential theft. But here's the best part about passkeys – they offer a great user experience.

Did you know?

Progressive Profiling

As a solution, some brands opt for progressive profiling – a concept in which data is collected gradually and transparently to avoid overwhelming the user. It uses shorter forms or surveys during multiple interactions to create detailed user profiles over time.

Set password → Collect data → Subscribe to newsletter → Auto login → Document consent

Login → Collect extra data → Store / update preferences

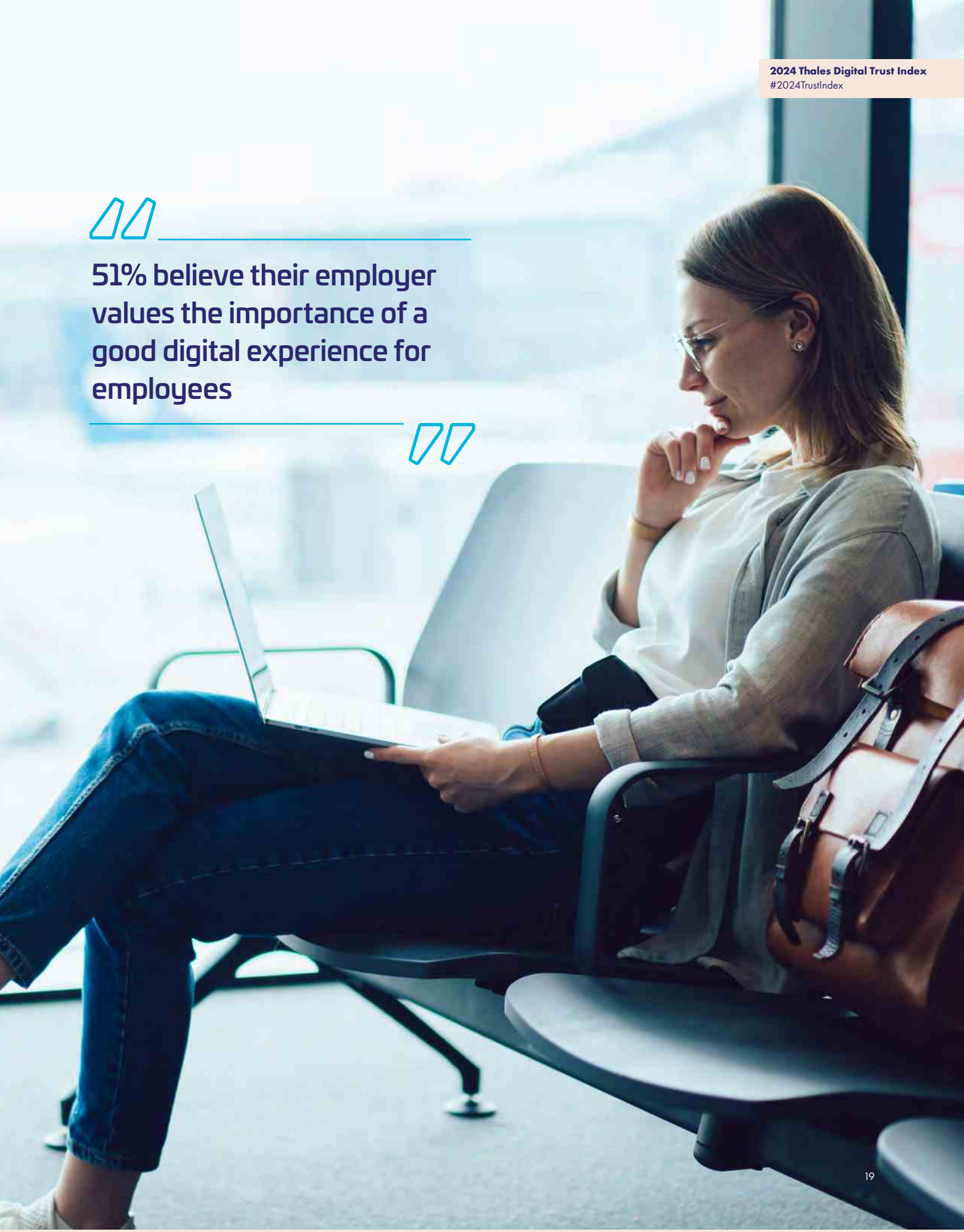
The Employee Experience

These same frustrations also extend to employees, with nearly half **(48%)** getting frustrated every time they have to create a new work password.

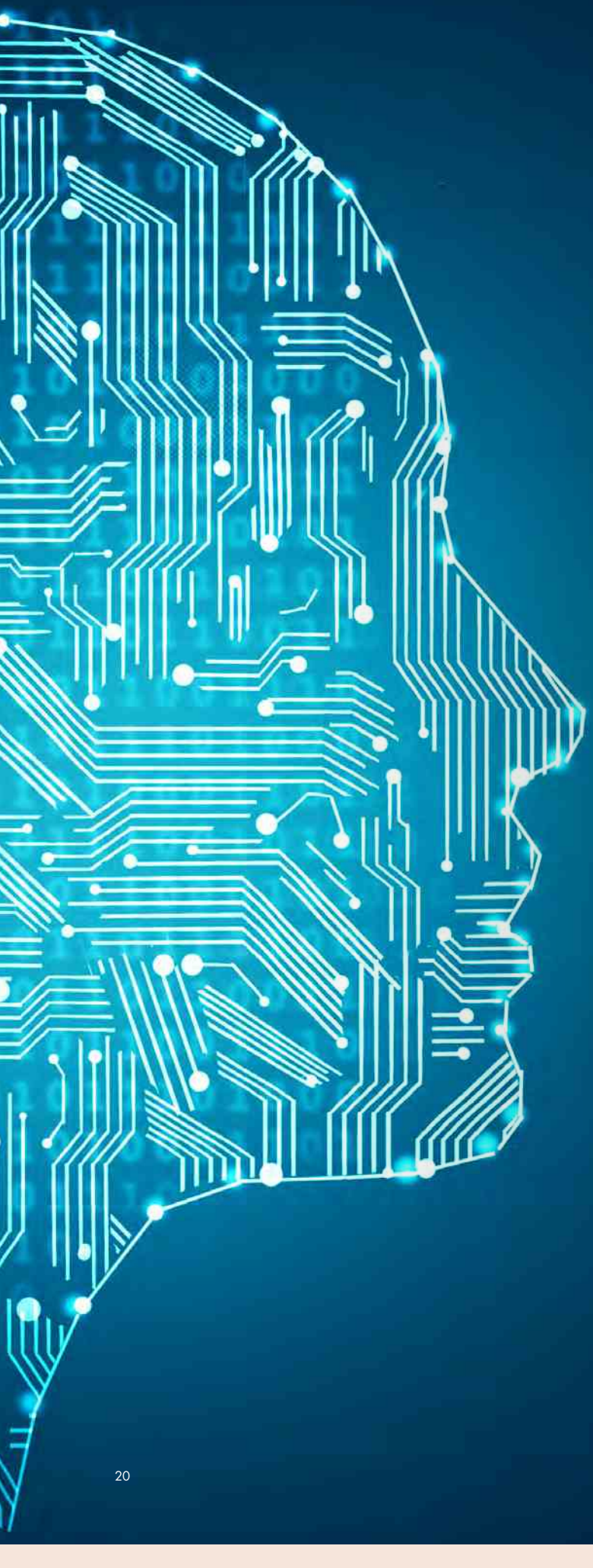
The way we work has changed on its head over the past decade. Ongoing digital transformation and global events such as the Covid-19 pandemic have meant that hybrid and remote working has fast become the norm for many businesses. However, despite millions of businesses across the globe allowing some form of hybrid or remote work, the experience for employees is not up to scratch.

Nearly half **(47%)** say that being able to work from home improves their productivity, but over a third **(36%)** say that it's too arduous to access their work profile to do so.

As it currently stands, just over half **(51%)** believe that their employer values the importance of a good digital experience for employees. Organizations need to adopt a holistic strategy for experience management, knowing how intricately connected customer experience (CX) and employee experience (EX) are for achieving transformational results. In essence, good employee experiences ultimately translate into good customer experiences.



51% believe their employer values the importance of a good digital experience for employees



TrUE stands for:

Transparent – Thales commits to explaining the rules by which its technology is deployed and designed, to the extent possible under the rules governing data confidentiality and protection of sensitive information,

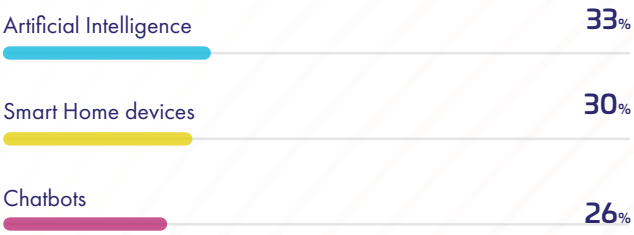
Understandable – Thales can explain and justify the use of the technology and the results, in such a way that users can understand the data used to arrive at a conclusion,

Ethical – meaning it follows objective standards protocols, complies with applicable laws, and promotes non-discrimination and equality

The Potential of Emerging Technology

As digital transformation continues apace, customers recognize that advancements in technology can be looked upon to help improve online experiences. Artificial Intelligence (AI) was perceived by consumers as the technology with the biggest potential to improve interactions with brands.

The top three technologies consumers feel will improve their online experiences



Generative AI has created a significant buzz over the past 12 months, thanks to the likes of OpenAI's ChatGPT and Microsoft Co-Pilot. The innovation and adoption of this technology has captured the public's attention, both good and bad, in terms of how our personal and working lives will be impacted.

Part of this debate has been around how brands will use generative AI in their interactions, and our study uncovered that over half **(51%)** of consumers would be happy for companies to use the technology to make their experiences better.

Fears around data security and privacy, however, are not to be ignored. Nearly six in ten **(57%)** global consumers are nervous that brands' use of generative AI will put their personal data at risk. Over four in ten **(43%)** said that they wouldn't trust any interactions powered by generative AI, and **47%** don't trust companies to use generative AI responsibly.

This contrasting viewpoints highlight the delicate balance that must be struck between experience and security, which is why businesses need to adopt what we call the TrUE Trust model to implementing technologies.

The TrUE technology approach has been designed by Thales to deliver responsible products and services that build trust for both users and service providers.

Adopting this approach will allow businesses to build trust for customers, all while adopting new technologies that will greatly improve user experience.

> **Nearly six in ten consumers are nervous that brands' use of AI will put their personal data at a risk.**

Country and Demographic Spotlights

Regulated sectors stand out as the most trusted sectors, in general, regardless of the country. But there isn't a clear winner, as the preferences and the extent of trust varies from one country to the other. Whether it's government services, healthcare, or banking, the sectors where customers around the world place the most trust in sharing their personal information are as follows:

Government Services


Singapore 61%


Australia 50%


Canada 49%


Netherlands 49%


UAE 46%

Healthcare


South Africa 50%


USA 38%

Banking

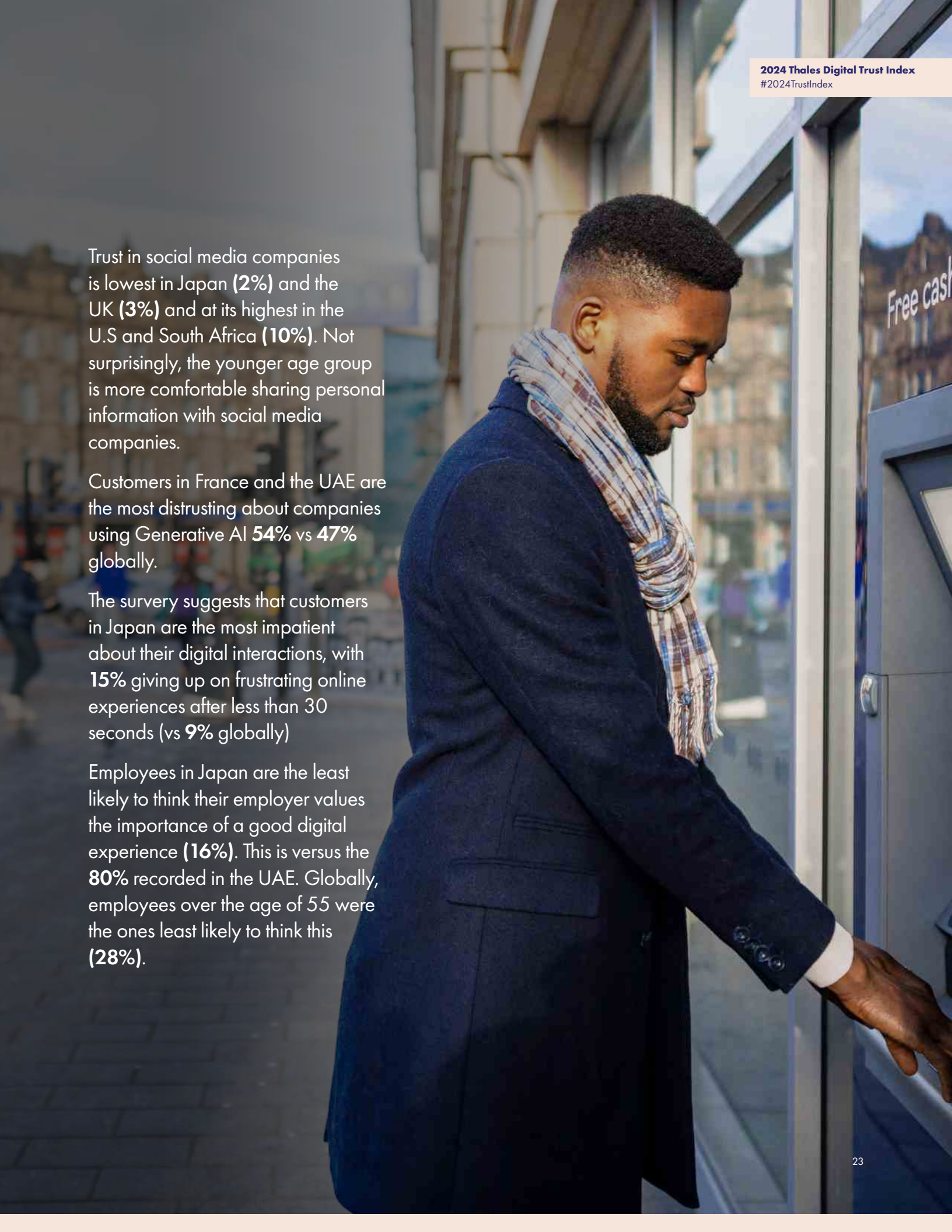

France 45%


UK 44%


Brazil 44%


Germany 43%


Japan 41%



Trust in social media companies is lowest in Japan **(2%)** and the UK **(3%)** and at its highest in the U.S and South Africa **(10%)**. Not surprisingly, the younger age group is more comfortable sharing personal information with social media companies.

Customers in France and the UAE are the most distrusting about companies using Generative AI **54%** vs **47%** globally.

The survery suggests that customers in Japan are the most impatient about their digital interactions, with **15%** giving up on frustrating online experiences after less than 30 seconds (vs **9%** globally)

Employees in Japan are the least likely to think their employer values the importance of a good digital experience **(16%)**. This is versus the **80%** recorded in the UAE. Globally, employees over the age of 55 were the ones least likely to think this **(28%)**.

Striking the Balance

There is no longer an either/or – customers want both security and seamless interactions. They're happy for data to be used, so long as they have control and visibility. Security is ultimately the point where friction can be introduced, but that no longer has to be at the expense of usability and experience.

We have identified a number of areas where businesses can introduce certain controls in the process to maintain the right balance between security and user experience. This includes:

Risk-based authentication (RBA): Not all situations call for stringent security. Risk-Based Authentication (RBA) dynamically adjusts the authentication level according to the situation, enabling businesses to strike a balance between security requirements and user experience without introducing excessive friction to the process.

Passkeys and passwordless authentication: The FIDO passkey revolution may just be in its infancy; however, it will soon become the norm. In the very near future, customers will expect a passwordless login experience – no matter the industry or service.

Progressive profiling: Customers only want to give their information when it's necessary. By employing a 'just enough, just-in-time' approach to data collection, progressive profiling is a compliant, consent-driven, and transparent method of gathering first-hand data. Giving customers the option to only share information as it's required will help grow trust without compromising on their end-user experience.

Bring Your Own Identity: By allowing individuals to use existing login credentials across multiple systems or applications, it increases convenience and gives users greater control over their online identities.

Consent & Preference Management: Privacy isn't just a mandate; it is becoming a differentiator for certain organizations. Businesses embarking on building digital products and services must weave the fabric of consent and preference management to ensure compliance and gain user trust.

Modern CIAM Solutions: Modern Customer Identity and Access Management solutions empower customers to have full control over their data, without compromising on experience. These solutions allow customers to automatically make SAR requests, sign up to services digitally, and even support third party login options.

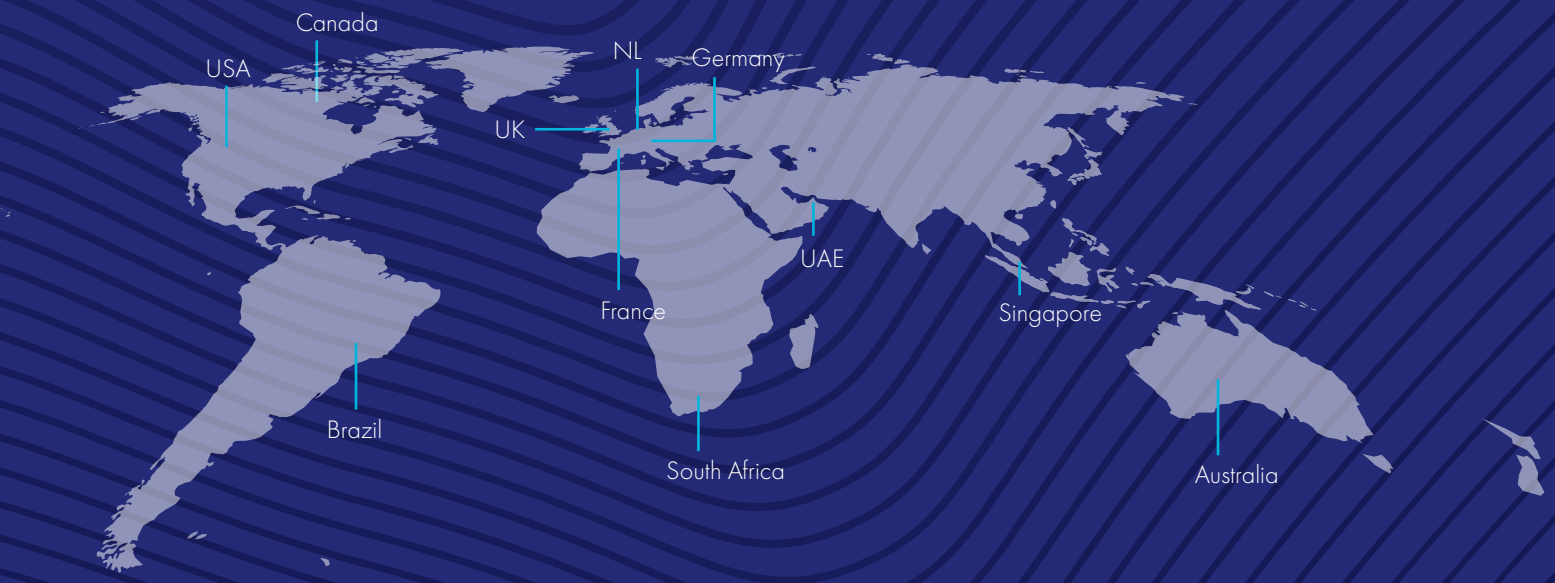
The relationship between trust and user experience is the cornerstone of successful online interactions. The imperative is clear: organizations must uphold an unwavering commitment to both data security and user experience to build a future where trust is the bedrock of digital interactions.

> **Customers want both security and seamless interactions.**

About the Research

Research was carried out among 12,426 general respondents in Australia, Brazil, Canada, France, Germany, Japan, Singapore, South Africa, The Netherlands (NL), the United Arab Emirates (UAE), the United Kingdom (UK), and the United States of America (USA).

Censuswide, who conducted the research, abides by and employs members of the Market Research Society which is based on the ESOMAR principles and are members of The British Polling Council.



THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/digital-trust-index