

2025

Endorsed by
kuppingercole
ANALYSTS

DIGITAL TRUST INDEX

Understanding How Digital
Experiences Affect Consumer Trust

Executive Summary

Trust is a two-way relationship. In today's digital age, it is hard to build and easy to erode. Last year's Digital Trust Index examined the delicate balance between a frictionless user experience, security, and the increasing importance of data privacy in shaping how trustworthy a brand is perceived to be. However, this year's findings reveal a significant shift: **consumers are currently shouldering the responsibility of building trust with brands.**

Consumers are required to navigate complex consent forms, ensure their data is protected, and constantly monitor for potential breaches. This situation underscores a substantial gap where brands need to step up and take proactive measures to earn and maintain consumer trust. Despite advancements, there is still too much friction for customers, as the user experience remains hindered by cumbersome processes and barriers. Global trust in digital services is decreasing or remaining stagnant at best, even among highly regulated industries. This trend highlights a growing scepticism and the need for brands to rebuild confidence.

The threat landscape does not remain stagnant. As cyber threats evolve, brands must continuously adapt their security measures to stay ahead. Customers are increasingly demanding that brands embrace innovative and advanced technologies to enhance both their experience and security. There is a clear demand for brands to adopt cutting-edge solutions that not only protect data but also streamline the user experience.

The responsibility of building and maintaining trust should not rest solely on consumers. Brands must take proactive steps to reduce friction, enhance security, and transparently communicate their efforts. By doing so, they can bridge the trust gap and foster a more secure and trustworthy relationship with their consumers.

Sponsored by





Global trust in digital services is decreasing or remaining stagnant at best, even among highly regulated industries.



Contents

Executive Summary	02
Key Findings	04
The Global Context	06
Consumer Privacy Demands	16
Brands' Growing Bad Bot Problem	21
Access Denied: Passwords Still a Problem	24
The Employee Experience	27
No Trade-Off: The Burden on Consumers	28
Building Trust Through Technology	30
Conclusion	32
About the Research	35

Key Findings



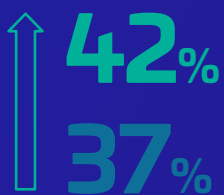
GLOBAL TRUST IN DIGITAL SERVICES IS IN DECLINE

The majority of sectors experienced a decline in trust levels compared to last year, with not one sector achieving at least **50%** when it comes to high levels of trust among consumers.



BANKING REMAINS THE NUMBER ONE TRUSTED SECTOR

Although this has dropped from 44% to just 32% of those aged 16-24.



Government organizations are the **only sector** where trust increased compared to last year (**42% vs 37%**).



NEWS MEDIA IS THE LEAST TRUSTED SECTOR



of consumers surveyed trust news media organisations with their personal data, placing them below all the other sectors.



CALLS FOR A PASSWORDLESS LOGIN EXPERIENCE ON THE INCREASE



Three-quarters of consumers indicated that passwordless authentication, such as using biometric data or a PIN, is important to them (versus 72% last year).



86% MORE THAN FOUR IN FIVE

consumers expect some level of privacy rights from the companies they interact with online.

19% NEARLY ONE IN FIVE

of consumers have been informed that their personal data has been compromised in the past year.



NO OTHER OPTION

37% of consumers forced to Share their Data

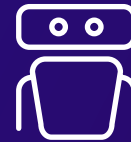


Underscoring a sense of compulsion rather than voluntary participation.

TOO MUCH ONUS ON THE CONSUMER

63% of consumers believe brands put too much onus on the consumer for data protection.

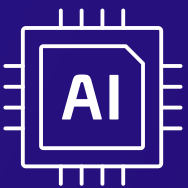
BOTS CAN RUIN BRAND REPUTATION



One in three consumers voiced frustration with ecommerce, directly caused by bad bots manipulating the customer purchasing process and ruining the customer experience.

THE USE OF INNOVATIVE AND ADVANCED TECHNOLOGIES

64% of consumers indicated that their confidence in a brand would significantly increase if they adopted emerging or advanced technologies that improves security and data protection.



33%

The Global Context

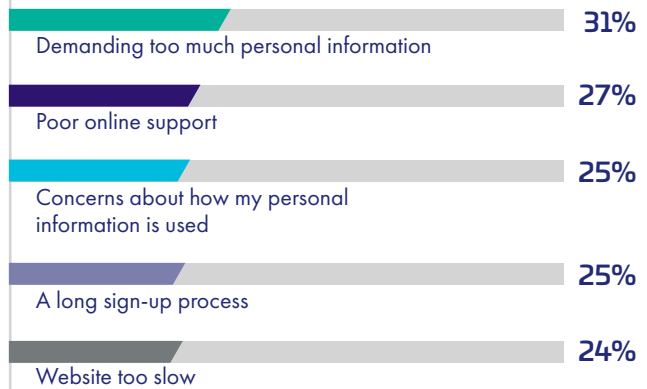
Organizations, no matter where they're based, or what industry they operate in, must protect customer data and offer a good customer experience. There's no space for either/or. Both are essential.

Trust has to be earned, and brands are not holding up their side of the bargain. In the past twelve months alone:

- 19%** of consumers have been informed that their personal data has been compromised
- 10%** More than one in ten consumers have had credit card or financial data stolen
- 28%** of consumers have experienced fluctuations in pricing for a product or service that they wanted to purchase
- 27%** More than a quarter of consumers have experienced downtime or slow service on a brand or service provider's website
- 13%** of consumers have been kicked out of an online queue for a service or product

Security, privacy and experience all ladder up to trust, so it's no wonder then that an overwhelming majority of consumers across the globe (82%) have abandoned a brand in the past 12 months.

The Top 5 Reasons Consumers Have Abandoned a Brand in the Past 12 month



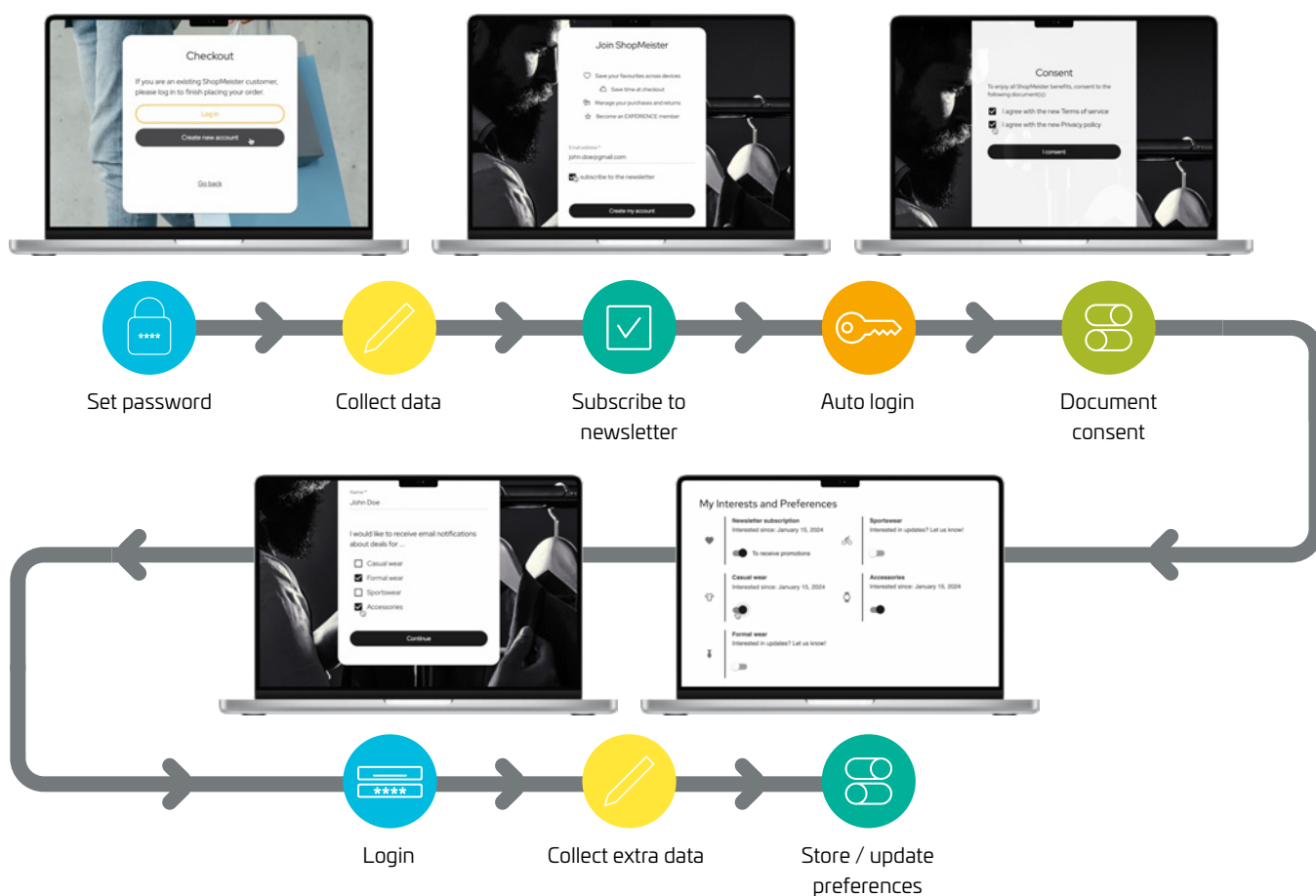
The Global Trust Index

Demanding too much personal information remains the number one trigger for consumers to abandon a brand in the past 12 months, with 31% of consumers stating that this was their top reason for letting go of a brand relationship.

Customers were asked which sectors they were most comfortable sharing their personal information with.














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.



2025 Trust Index Ranking

Which sectors do you trust the most when it comes to sharing your personal information?

1 st		Banking	44%
2 nd		Government	41%
3 rd		Healthcare	40%
4 th		Insurance	24%
5 th		Education	17%
6 th		Hospitality	7%
7 th		Transportation (airlines, trains, etc)	6%
8 th		Retail	5%
8 th		Entertainment	5%
9 th		Social Media Companies	4%
9 th		Automotive	4%
9 th		Logistics	4%
10 th		News media organizations	3%

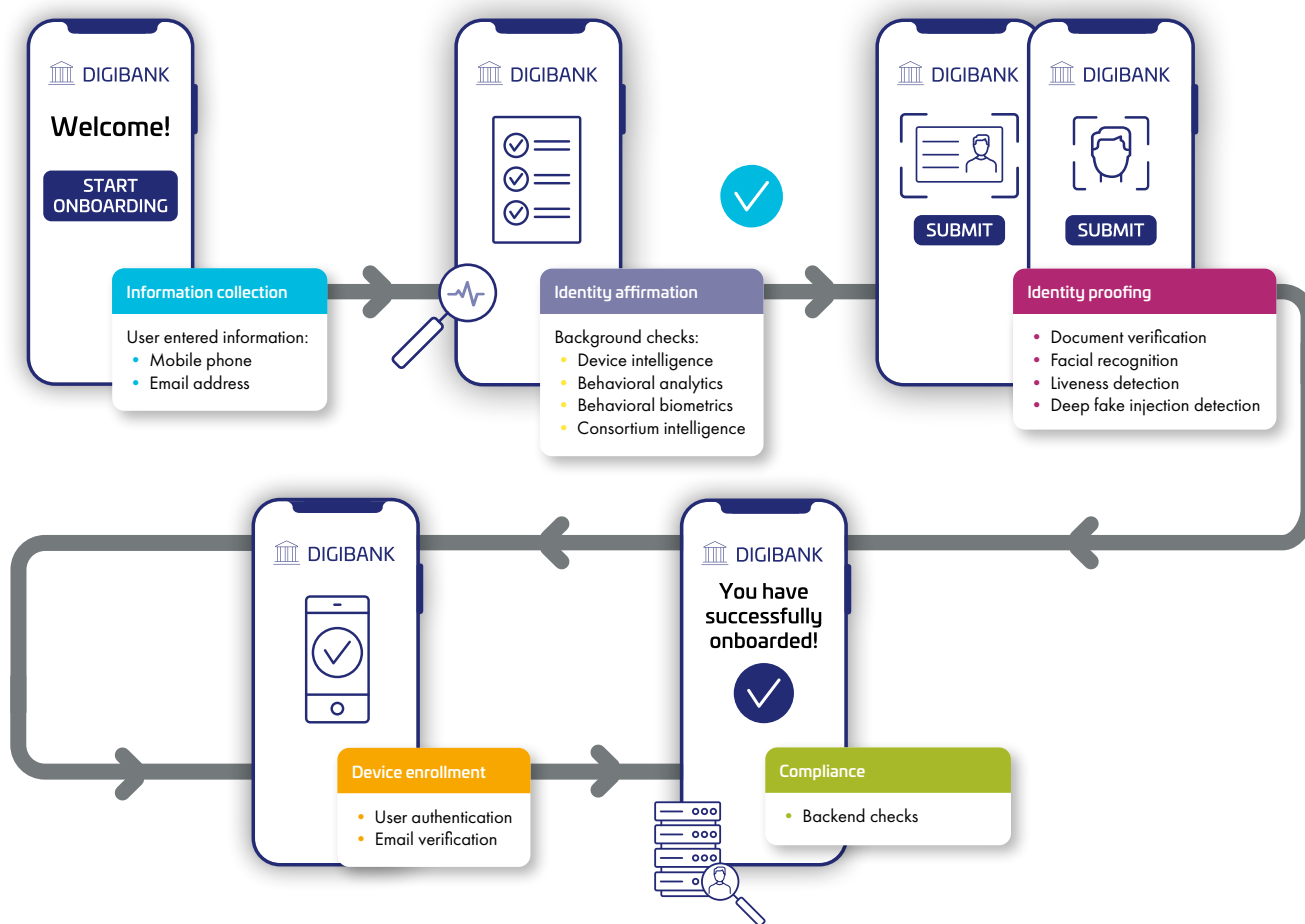
Global Trust in Digital Services is Declining

Overall, the findings point to a universal decline in trust for digital services, with most sectors experiencing a decline compared to this time last year, or at best remaining stagnant.

When it comes to protecting their personal data, the most trusted industries by consumers are banking, government services and healthcare. The higher levels of trust in these regulated industries mirrors the trend we saw last year. However, even among these highly regulated industries, not one of these sectors has managed to earn the highest level of trust of even half of their customers – highlighting the tremendous amount of work that still needs to be done by these industries.

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.



Regulations impacting the banking sector

Despite there being a long way to go, banking once again tops the trust index, in part down to the levels of regulation underway, designed to both enhance user experience and safeguard data.



Digital Operational Resilience Act (DORA):

The European Union (EU) regulation, effective from January 2025, aims to strengthen the IT security and resilience of financial entities, including banks and insurance companies. DORA ensures that these entities can withstand severe operational disruptions by harmonising rules related to Information and Communication Technology (ICT) risk management... risk management, third-party risk, and incident reporting.



Payment Card Industry Data Security Standard (PCI DSS 4.0)

Coming into effect on March 31 2025, PCI DSS 4.0 is a new global standard specifically designed to protect cardholder data. It includes 12 key requirements, such as installing network security controls, protecting stored account data, and regularly monitoring and testing networks. The latest standard has been specifically designed to address emerging threats and technologies. One of the key updates in PCI DSS 4.0 is the enhanced multi-factor authentication (MFA) requirements to further secure access to cardholder data environments.



Third Payment Services Directive (PSD3):

Introduced in June 2023, PSD3 updates the framework for electronic payments in the EU. It focuses on enhancing competition and innovation while ensuring consumer protection.

Key aspects include stronger customer authentication, improved fraud prevention, and better access to payment systems for non-bank providers.

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



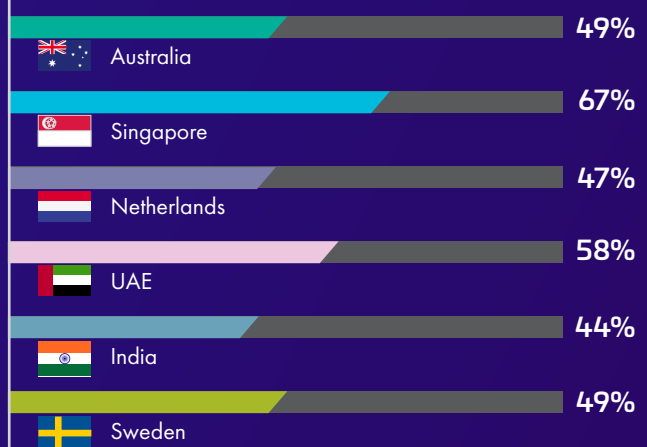
Inherence

Banking remains number one trusted sector

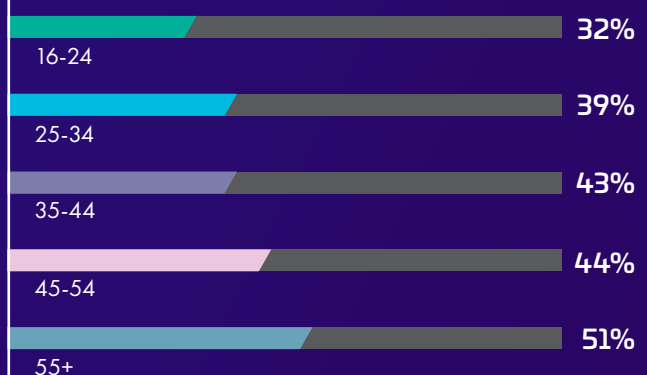
While banking globally ranks number one, there are some key demographic splits:

- Consumers surveyed aged 55+ are most likely to trust the Banking sector most when it comes to sharing their personal information, compared to those aged 16-24, who are least likely to trust this sector the most (**51% vs 32%**).
- Instead, consumers surveyed aged 16-24 are more likely to trust the Government (**35%**) and the Healthcare sector (**35%**) most.
- In the USA, Healthcare was more trusted – marginally at **41%**. Trust in Government is overall a lot lower than the average at **29%**.
- In Australia, Singapore, Netherlands, UAE, Sweden and India, the Government was most trusted.

Counties where Government is the most trusted



Trust in Banking - Broken down by age



The Outlier: Trust in Government Increases

Compared to last year, the only sector to see an increase in trust overall, was that of Government services – with a 5% increase on 2024, overtaking healthcare on the overall global rankings list.

Citizens increasingly want access to digitized services, and by that same token rolling out these services helps governments increase efficiency, reduce costs and improve accessibility for citizens. A great example of this in action is the roll out of digital driver's licenses (DDLs), in Queensland Australia.

Did you know?



Since its launch in late 2023 by the Queensland Department of Transport and Main Roads (TMR), over 500,000 Queenslanders have downloaded the new Digital License app developed by Thales and local partners, Code Heroes and Aliva. Developed with security and privacy at the core, Thales' Digital ID Services Platform powers the app and provides a cybersecure home for users' identity data.

With core technology provided by Thales, supported by development and operations from local partners Code Heroes and Aliva, the QLD Digital Licence app is simple to use, secure, and designed with data security and user privacy in mind. The app includes features such as multi-factor authentication, integration with the Queensland Digital Identity (QDI) service, and built-in verification for secure user-to-user information exchange. The app's consent-based design gives the individual control over their identity data – users can present or share information from the app by selecting from common use cases that disclose only the relevant information for the transaction, such as 'proof of age', which displays an 'over 18' screen without exposing date of birth, address, or driving information – a popular feature.

Trust in News Media Organizations

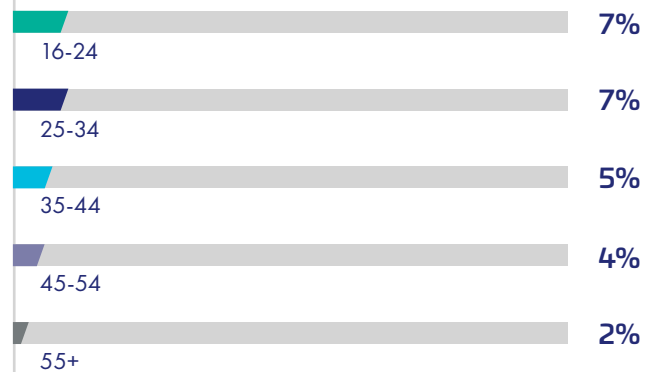
News media organizations are at the bottom of the trust index when it comes to consumers sharing their personal information. Only 3% of consumers surveyed trust news media organizations with their personal data, placing them below all the other sectors.

The proliferation of misinformation and the increasing sophistication of deep fake technology have significantly eroded public trust in news media. Consumers are becoming more skeptical about the authenticity of the information they consume, leading to a general distrust of the platforms that disseminate this information. The same can be said for social media platforms, which experienced a 33% drop in trust compared to last year.

Social media platforms only score marginally higher on the index, with 4% - although there are higher levels of trust among younger age groups.

Regardless of the industry, businesses must comply with international data privacy regulations. However, sectors lower in the rankings have faced fewer specific directives concerning data security and privacy. These lower-ranked sectors should consider adopting best practices from more trusted and highly regulated industries. Building this trust is essential for encouraging customers to share their data, ultimately enhancing their overall experience.

Trust in social media companies - by age



Did you know?

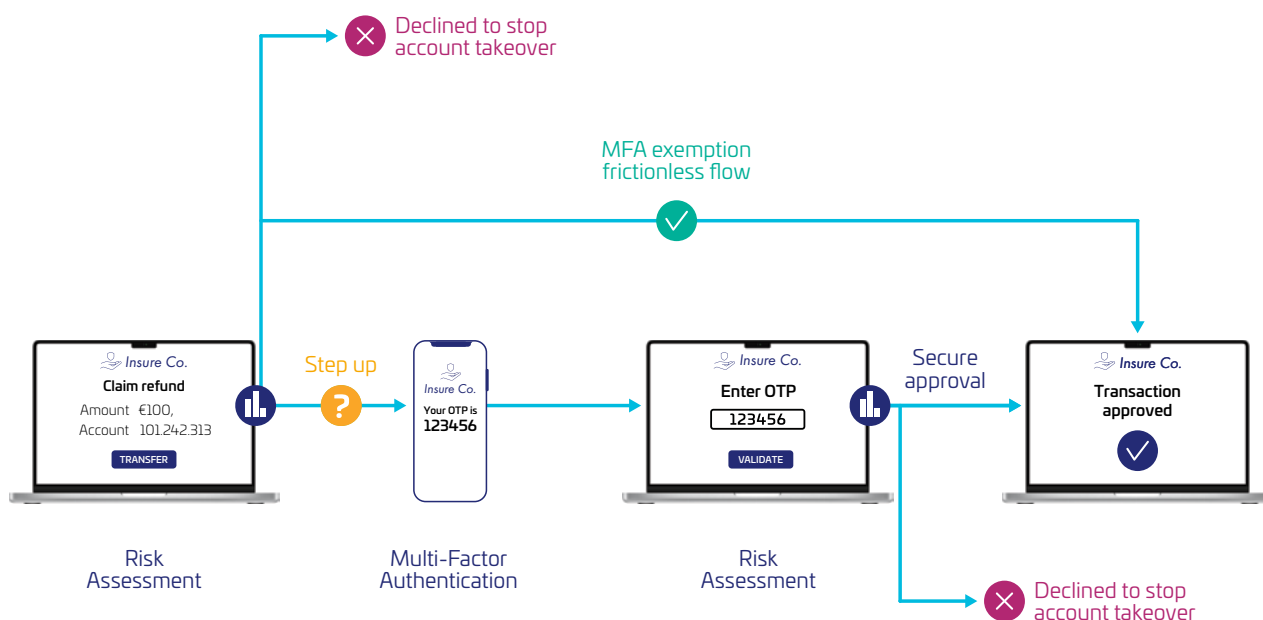
Meta, the parent company of Facebook and Instagram, has decided to get rid of independent fact-checkers. Instead, the company will rely on a user-based system known as "Community Notes" to report false stories and misleading information. This move has sparked concerns about the potential spread of misinformation – potentially further erasing trust in these platforms.



Did you know?

Risk-Based Authentication (RBA)

Risk-Based Authentication (RBA) is a type of authentication that varies based on certain behaviors 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 behavior. 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.



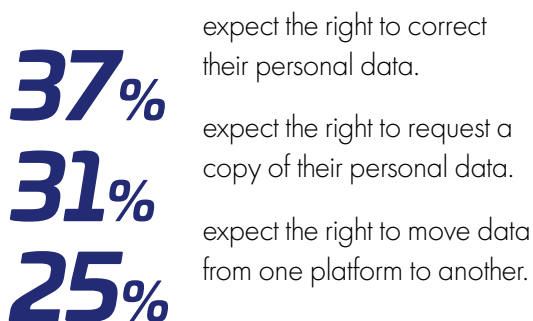
This simple RBA example depicts how authentication can be made more frictionless and more secure. RBA runs in the background, evaluating when and if, “stepping up” to a stronger form of authentication is necessary.

Consumer Privacy Demands

Demanding too much personal information may be the number one cause of consumers abandoning a brand, but that doesn't mean they're against sharing their data under the right circumstances.

Most customers (89%) are willing to share their data with organizations, but that comes with some non-negotiable caveats. More than four in five (86%) expect some level of privacy rights from the companies they interact with online. This is consistent with the findings from the 2024 research.

The most in-demand expectation is the right to be informed that their personal data is being collected (52%), and the right to have their personal data erased (53%). When asked about other privacy rights:



These expectations extend to when a customer stops using a brand or service. 49% of people would not be comfortable if a brand continued to have access to their data after stopping to use a product or service, and just 19% said they feel comfortable because they believe their data will be used for legitimate reasons.

Did you know?

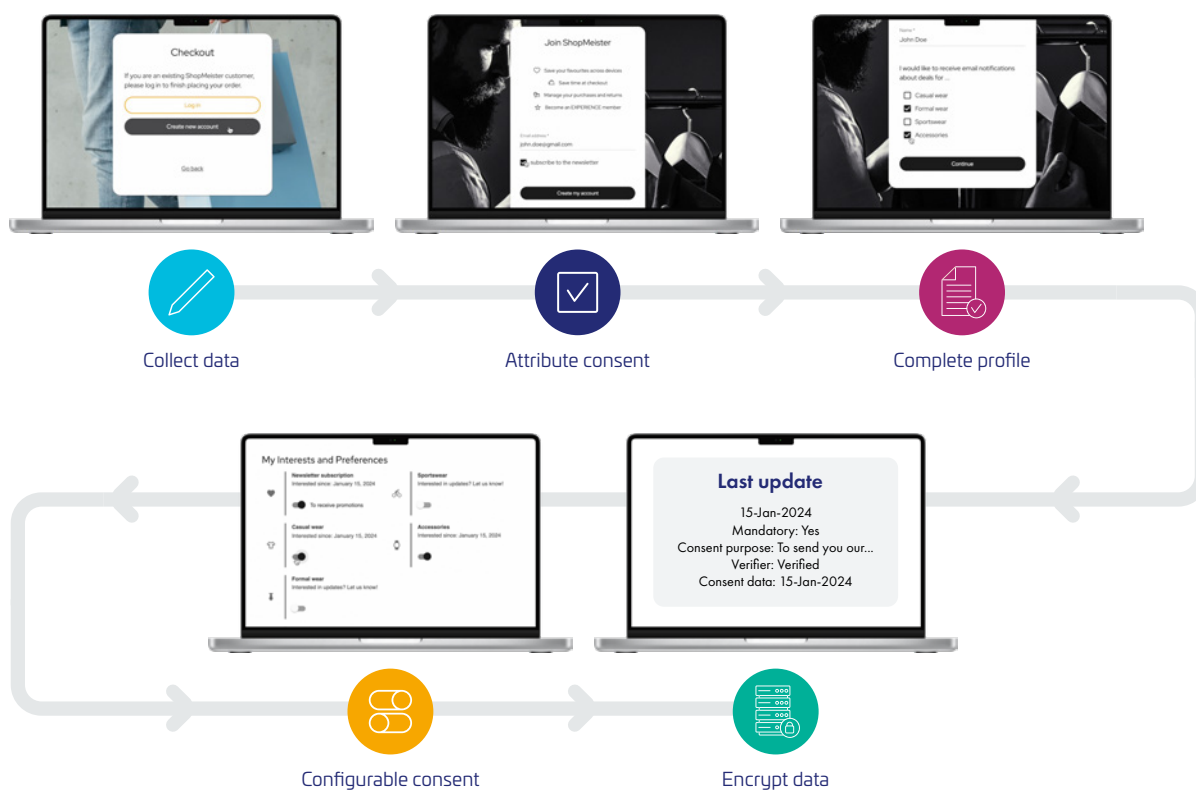
Canada's Consumer Privacy Protection Act (CPPA): Proposed to replace PIPEDA, the



CPPA aims to modernize Canada's data privacy framework. It introduces stricter consent requirements and enhanced rights for individuals to access and control their personal data.

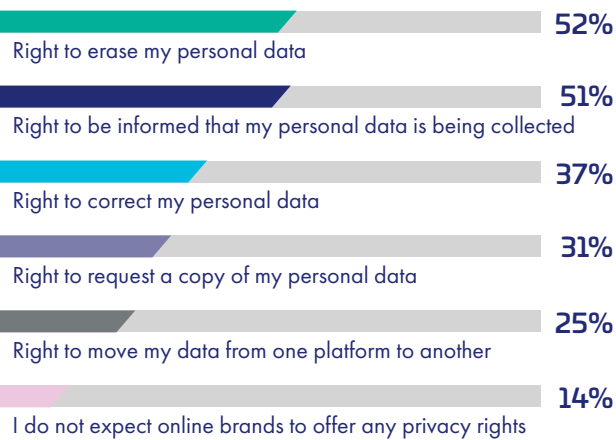
Data Subject Requests

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.

The privacy rights consumers expect



Did you know?

Brazil's General Data Protection Law (LGPD): Similar to the GDPR, the LGPD provides comprehensive data protection rights to Brazilian citizens. It includes provisions for data access, correction, and deletion, and has seen increased enforcement actions in recent years.

“

The GDPR continues to be a benchmark for data privacy laws worldwide. It grants individuals the right to access their personal data, request corrections, and demand deletion.

”



Did you know?

India's Digital Personal data Protection Act (DPDP): Effective from August 2023, the DPDP Act aims to protect the personal data of Indian citizens. It regulates data processing activities, ensuring individual's rights to access, correct, and delete their data. The DPDP Act also includes provisions for managing ICT risks, third-party risks, and incident reporting, enhancing the overall data security and resilience of organisations operating in India.



What is a Bot?



A bot is an automated software application that performs tasks on the internet. Bots can be good, such as search engine crawlers that index content, or bad, such as those used for malicious activities.

What is a Bad Bot?



Bad bots are automated programs designed to perform harmful activities, such as scraping data, spamming, and launching denial-of-service attacks. These bots can mimic human behaviour, making them difficult to detect and block.

“

67% have experiences online disruption in the past year

”

Brands' Growing Bad Bot Problem

Data privacy is just one piece of the puzzle that forms the foundation of consumer trust, with online experiences playing a huge role in shaping perception of (and trust in) a brand. After all, poor online support was highlighted as the second most common reason behind brand abandonment in the past twelve months.

Nearly half of all internet activity is now driven by bots. With a third of this traffic coming from malicious or 'bad' bots.

Account Takeover Bots: A form of identity theft in which bad actors gain illegal access to user accounts. Account Takeovers can be performed using several types of automated threats, predominantly Credential Stuffing (mass log in attempts used to verify the validity of stolen username/password pairs) and Credential Cracking (identifying valid login credentials by trying different values for usernames and/or passwords).

Scalping Bots: Scalping is the act of obtaining limited-availability and/or preferred goods and services by unfair methods for the purpose of reselling them at a higher price point to make a profit.

Carding and Card Cracking Bots: Bots are being used to verify stolen credit card numbers by making multiple small payments (Carding) or trying to identify missing information like expiry dates and CVV numbers (Card Cracking). They directly hurt the fraud score of businesses as well as increase customer service costs in order to process fraudulent chargebacks.

Spamming Bots: These bots are being used to spread fake news, propaganda and even post fake reviews to blemish rival products. They are also being used to hide malicious content, like malware, inside click-bait links.

Why Bots are a Problem for Brands

Bad bots pose significant challenges for brands, including:



Security Risks

Bad bots can compromise the security of websites and applications, leading to data breaches and other cyber threats.



Operational Costs

Dealing with bad bots can increase operational costs due to the need for additional security measures and resources to manage bot traffic.



Customer Experience

The presence of bad bots can degrade the user experience, causing frustration and loss of trust among customers.

While the prevalence of malicious bots can have far reaching security and privacy implications, they can also create havoc for consumer' end-user experience. When asked what had made them lose their patience online in the past twelve months:

- 28%** of consumers have lost their patience online due to having to take part in a CAPTCHA test to prove they are not a bot.
- 27%** have been frustrated by being in long online queues.
- 14%** have been annoyed by dynamic pricing.

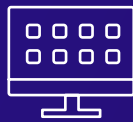
Why Brands Need Bot Protection Strategies

Implementing bot protection strategies to safeguard consumer trust and ensure a positive online experience. Effective bot protection can help brands:



Enhance Security

Protect against data breaches and other cyber threats by detecting and blocking malicious bot traffic.



Improve User Experience

Reduce the need for CAPTCHA tests and long online queues, leading to a smoother and more enjoyable customer journey.



Reduce Costs

Lower operational costs by minimizing the impact of bad bots on website performance and security.

“

Investing in robust bot protection strategies is essential for brands to maintain consumer trust and deliver a secure, seamless online experience.

”

Access Denied: Passwords Still a Problem

An overwhelming majority of consumers (87%) have lost their patience online in the past twelve months.

Top reasons for consumers losing their patience:

1 st	Advertising pop-ups	38%
2 nd	Password re-sets	31%
3 rd	Having to re-enter personal information when I have used the brand before	28%
4 th	Having to take part in a CAPTCHA test to prove I'm not a bot	28%
5 th	Being in long online queues	27%
6 th	Chatbots	24%
7 th	Complex cookie options	23%
8 th	Having to enter payment details	18%
9 th	Banking verification	17%
10 th	Dynamic pricing	14%
11 th	Brands that I have used before forgetting my online preferences	14%

Issues around identification and verification continue to be a huge source of friction, and frustration for consumers – with password re-sets, having to re-enter personal information, and brands forgetting online preferences causing online outrage.

Despite calls for passwords to be abolished, they remain a commonly used means of authentication. However, they continue to frustrate consumers, leading to brand abandonment.

- **Password Frustrations:** Despite increased calls for password dependency to be abolished, more consumers abandoned a brand in the past 12 months due to forgetting their password (17% this year versus 16% last year). Additionally, 16% cited the need to create long and complex passwords as a reason for switching brands.
- **Impact on Brand Loyalty:** Password-related issues are among the top factors causing consumers to abandon brands. Specifically, 18% of consumers mentioned the requirement to create long, complex, and unique passwords as a major deterrent.

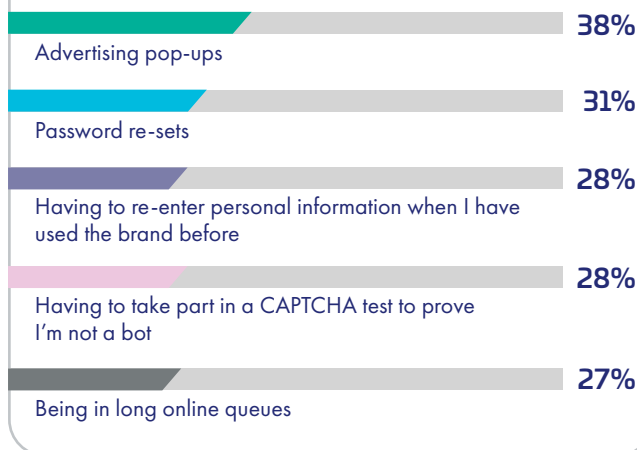
These findings highlight the ongoing challenges consumers face with password management and the significant impact on brand loyalty. As brands strive to improve user experience, addressing password-related frustrations could be a key area of focus.

“

91% of 16-25 year olds have lost their patience online vs 82% of over 55s

”

Impatience Index - The Top Five Issues that Make Consumers Lose Their Patience Online



Call for Passwordless and Multi-Factor Authentication:

- **Passwordless Authentication:** Calls for a passwordless login experience have increased this year, with three-quarters (75%) of consumers indicating that passwordless authentication, such as using biometric data or a PIN, is important to them (versus 72% last year). Over a third (35%) stated that this feature is very important.
- **Passkeys:** Passkeys are emerging as a secure and user-friendly alternative to traditional passwords. They use cryptographic keys stored on a user's device, providing a seamless login experience without the need to remember complex passwords. In fact, 48% said they would trust a brand more if they implemented passkeys.
- **Multi-Factor Authentication (MFA):** Almost 9 in 10 (86%) consumers emphasized the importance of having MFA for additional security on their online accounts, compared to 81% last year. Half (50%) of the respondents rated this feature as very important.

These findings suggest a growing consumer preference for more secure and user-friendly authentication methods. Implementing passwordless and multi-factor authentication could significantly enhance user satisfaction and reduce brand abandonment.

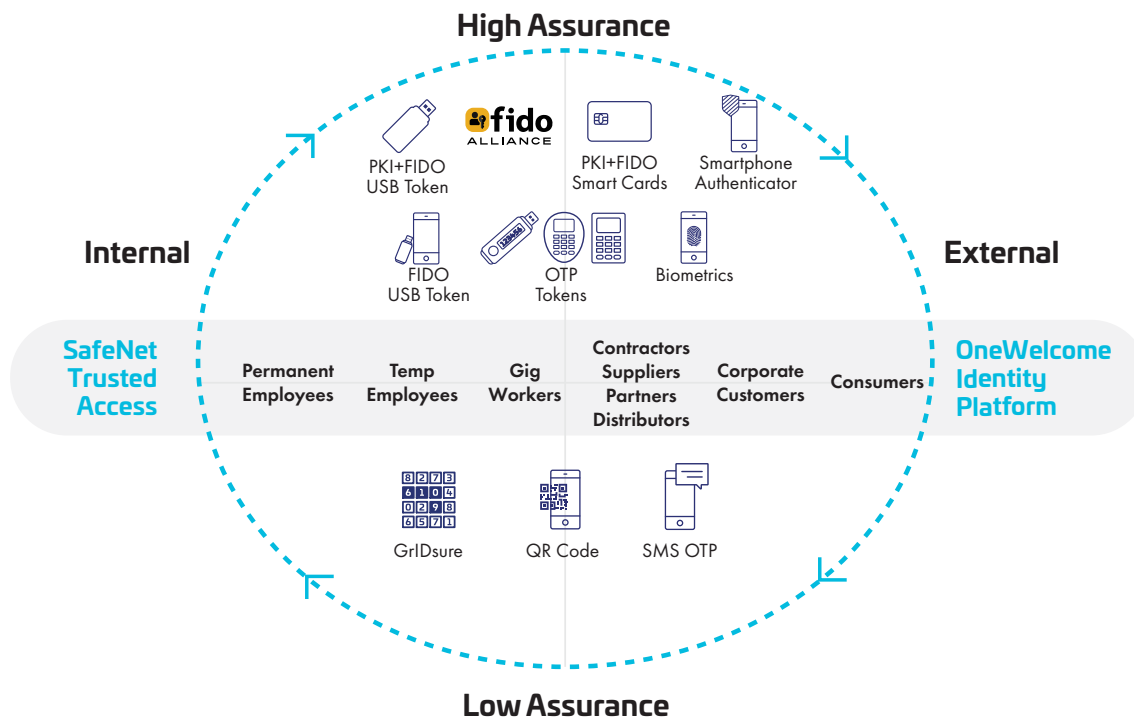
The good news is that companies can strike the perfect balance by using risk management technologies that run silently in the background to introduce risk-based authentication (RBA) / adaptive MFA. By implementing this, a brand can minimize friction by only asking for additional authentication when the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

Did you know?

Passwordless 360° has been designed to provide passwordless authentication across various user types and assurance levels.

Thales Passwordless 360° is a comprehensive solution designed to provide passwordless authentication across various user types and assurance levels.

- **Broad Coverage:** It supports multiple types of users, including employees, customers, business partners, and suppliers, ensuring a wide range of applications.
- **Modern Technologies:** The solution incorporates the latest technologies like FIDO passkeys, biometrics, and hardware security keys, while also leveraging existing investments in passwordless technologies.
- **Enhanced Security:** By eliminating traditional passwords, it reduces security risks associated with password theft and phishing.
- **User Experience:** It offers a seamless and frustration-free login experience, improving user satisfaction and reducing the need for password resets.
- **Risk-Based Authentication:** Thales Passwordless 360° includes risk-based authentication (RBA) and adaptive multi-factor authentication (MFA), which only require additional authentication when the risk is high.



The Employee Experience

As hybrid working becomes the new normal, businesses must focus on building trust not only with consumers but also with employees. Ensuring that employees have a seamless and secure digital experience is crucial for maintaining productivity and job satisfaction.

The link between remote working and productivity is on the increase, with 56% of employees stating that it improves their productivity, compared to 47% last year. This highlights the importance of seamless and efficient remote access solutions.

However, the findings reveal that it's becoming increasingly harder for employees to work productively and access what they need, particularly when working remotely.

It's becoming harder to work remotely: 41% of workers believe that the process to access their work accounts remotely is too arduous, compared to 36% this time last year. Current security measures and login procedures may be overly complex or time-consuming.

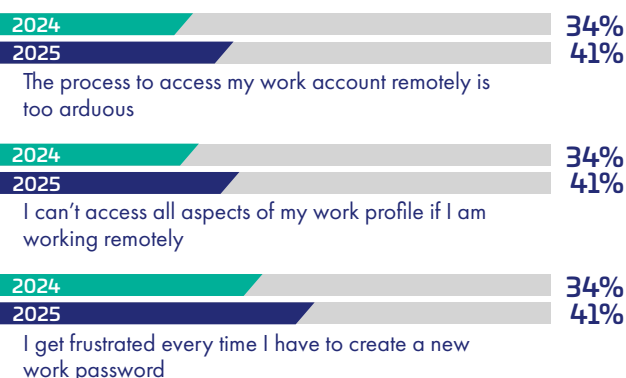
Complexity is causing decreased productivity:

56% of employees get frustrated every time they have to create a new work password, compared to 48% last year.

Impact on day to day working: 42% of workers report that they cannot access all aspects of their work profile when working remotely, which can hinder their ability to perform their job effectively. This friction has increased compared to last year, with 37% reporting this issue in 2024.

Interestingly, 57% of employees feel that their employer values the importance of a good digital experience for employees, while 9% disagree, with this figure rising to 13% among workers in Germany. This suggests that while many employers are making efforts to improve digital experiences, there is still a significant portion of the workforce that feels their needs are not being fully met.

It's getting harder for employees



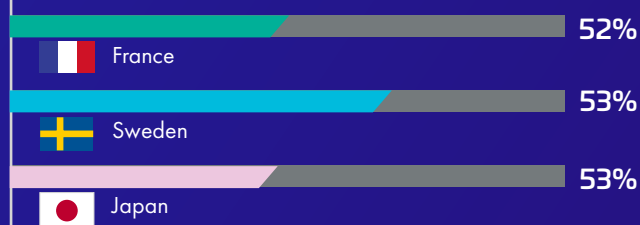
No Trade-Off: The Burden on Consumers

In today's digital age, the exchange of personal data for services has become a common practice. However, this transactional nature of data exchange is fraught with challenges. The core issue lies in the perceived lack of benefit and transparency. Consumers often feel coerced into sharing their data without a clear understanding of how it will be used, leading to significant distrust. 45% of consumers do not trust this growing brand practice, with distrust levels peaking at 57% among consumers in France.

Lack of Perceived Benefit

The statistics highlight a critical gap in communication and trust between brands and consumers. For instance, 37% of consumers only share their data because they have no other option, underscoring a sense of compulsion rather than voluntary participation. This sentiment is further exacerbated by the 33% of global consumers who do not understand how their data is managed, pointing to a dire need for better transparency.

Countries with the lowest levels of understanding about how their data is used

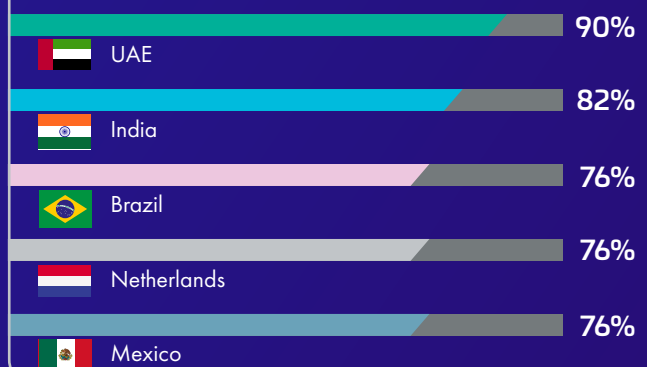


Too Much Onus on the Consumer

A significant portion of consumers believe that brands place too much responsibility on them when it comes to protecting personal data. The findings show that:

- 63% of consumers believe brands put too much onus on the consumer for data protection.
- This sentiment is even stronger in certain regions, with 75% of consumers in Brazil and India, and 78% in the UAE, agreeing with this statement.

Countries with the highest levels of understanding about how their data is used



Implications for Brands

The growing trend of requiring data exchange for services, coupled with the lack of transparency and the heavy burden placed on consumers, is eroding trust. Brands need to recognize that customers are increasingly aware of their data privacy rights and are demanding more control and understanding over how their data is handled.

To rebuild trust, brands must:

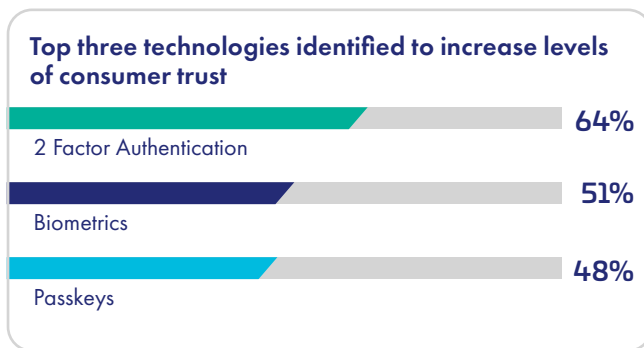
- **Enhance Transparency:** Clearly communicate how consumer data is collected, used, and protected.
- **Reduce the Burden:** Implement user-friendly data protection measures that do not place excessive responsibility on the consumer.
- **Build Trust:** Demonstrate a commitment to data privacy and security through robust protection strategies and transparent practices.

By addressing these concerns, brands can foster a more trusting relationship with their customers, ultimately leading to a better online experience and increased loyalty.



Building Trust Through Technology

The integration of advanced technologies plays a crucial role in enhancing consumer trust in brands.



Multi-Factor Authentication (MFA)

64% of consumers surveyed would trust a brand more if it used MFA. This technology adds an extra layer of security, ensuring that even if passwords are compromised, unauthorized access is prevented.

Brands that implement MFA can differentiate themselves by demonstrating a commitment to protecting user data, which is particularly important in an era of frequent data breaches.

Biometrics:

Over half (51%) of the respondents indicated increased trust in brands that use biometric authentication. Biometrics, such as fingerprint or facial recognition, provide a secure and convenient way to verify identity, reducing the risk of fraud.

The convenience and security offered by biometrics make it a popular choice among consumers. Brands that adopt biometric authentication can enhance user experience while simultaneously bolstering security, leading to higher trust levels.

Passkeys:

48% of consumers would trust a brand more if it used Passkeys. Passkeys eliminate the need for traditional passwords, which are often vulnerable to breaches, by using cryptographic keys that are unique to each user.

The move towards Passkeys reflects a shift in consumer expectations for security. By adopting this technology, brands can reduce the risk of password-related breaches and build a reputation for being at the forefront of security innovation.

Digital Sovereignty:

37% of consumers expressed greater trust in brands that implement digital sovereignty measures. This approach ensures that data is stored and processed within specific jurisdictions, complying with local data protection regulations.

Digital sovereignty addresses growing concerns about data privacy and regulatory compliance. Brands that prioritize this can appeal to consumers who are increasingly aware of and concerned about where and how their data is handled.

Generative AI and AI:

Approximately 32-33% of consumers would trust a brand more if it used generative AI or AI. These technologies can enhance personalization and security, making interactions more efficient and secure.

The use of AI can significantly improve customer service and personalization, leading to a more tailored and satisfying user experience. Brands that leverage AI effectively can build stronger relationships with their customers by meeting their specific needs and preferences.

Use of Innovative and Advanced Technology Can Build Trust

The incorporation of innovative and advanced technologies by businesses plays a crucial role in enhancing consumer confidence regarding the protection of sensitive data. 64% of consumers indicated that their confidence in a brand would significantly increase if they were aware that such technologies were being utilized. This underscores the critical importance of transparency and the proactive adoption of state-of-the-art security measures.

By openly communicating their commitment to these technologies, businesses can effectively build and maintain trust with their consumers, thereby fostering a more secure and trustworthy relationship.

Global decrease in digital trust is not only quantifiable, but preventable

Conclusion by John Tolbert, Director of Cybersecurity Research at KuppingerCole Analysts

This survey shows metrics that should be alarming to enterprises that conduct business online. The global decrease in digital trust is not only quantifiable, but preventable. The study shows that the banking sector, while far from having stellar trust numbers, leads other industries in digital trust. Banks have understood the need for security since the days of physical security only – safes, vaults, lockboxes, teller alarms, cameras, etc. Banks are highly motivated to protect their assets and their reputations. It's key to their business. Financial institutions and payment service providers outside of banks should implement customer security measures to match the level of protection afforded by banks. Other industries are playing catch up when it comes to online security, and many have a long, long way to go.

Healthcare remains relatively high in digital trust, despite the onslaught of ransomware attacks that have plagued healthcare companies and interrupted healthcare delivery over the last few years. Hospitals, clinics, and health insurers have been breached and have lost patient medical records en masse, which typically erodes trust when it happens to organizations in other sectors. However, healthcare is a fundamental part of everyday life, so it's possible we're seeing trust borne out of necessity and lack of choice. Healthcare may remain isolated from the loss of public trust for now but should not rely on that for a long-term strategy. Healthcare organizations must get serious about cybersecurity to prevent ransomware and malware-less ransom attacks, as well as take steps to improve customer front-end security and privacy.

Travel and hospitality, retail, and entertainment sectors are suffering from low trust ratings also. Companies in these areas should conduct thorough usability engineering studies and exercises. Talk to users. Find out what they want in terms of interacting with their digital properties. Find out what it takes first-hand to increase digital trust with their brands. Passwordless authentication, right-sized PII collection, transparency about PII usage and sharing, and options to edit and delete PII would of course go a long way toward building that trust.

“

Bot detection and management are no longer “nice to haves”. Bad bots are interfering with legitimate user traffic on unprotected sites, which leads to less engagement and less revenue

”

Social media companies transact PII as a means of doing business. Placing the cost of user verification on the users themselves will not help that much in the long run. News media organizations rank the lowest in this survey. This is unfortunate, but the ad-based revenue model, declining subscriptions, and partisan political alignments have changed the nature of reporting at some outlets. Social and news media organizations should embrace both

security enhancements for their users and fact-checking to demonstrate integrity and improve their perception to enhance trust.

As mentioned in this Trust Index, multifactor, passwordless, and risk-based authentication (RBA), if implemented correctly can boost security and lead to better customer engagement. No one likes passwords. Everyone knows passwords are insecure. But SMS OTP is really not any better in terms of security, and it leads to an even worse consumer experience. FIDO paskeys offer better, unphishable means of logging in, and are more acceptable to users. Risk-based authentication adds a nearly invisible layer of protection that knowledgeable users prefer. All three of these authentication paradigms are readily available in CIAM solutions today. Many CIAM solutions combine a variety of authentication factors to make it easier for deploying organizations to choose options that best suit their user base. If your organization is not making full use of passwordless MFA and RBA, make implementing better authentication a top priority for 2025.

Many customers value privacy in transactions. It is essential in banking, healthcare, and other industries. Be transparent with privacy policies and adhere to them. Allow customers to change and remove data as desired. Provide granular PII sharing options – providing “all or nothing” options will hurt the bottom line.

Bot detection and management are no longer “nice to haves”. Bad bots are interfering with legitimate user traffic on unprotected sites, which leads to less engagement and less revenue. Full-featured Fraud Reduction Intelligence Platforms (FRIP) incorporate sophisticated bot detection and management, most often based on invisible-to-the-user behavioral biometrics, that can deter malicious bots and allow for supervised processing of non-malicious bots. FRIP solutions are a vital adjunct to CIAM systems that both improve the customer experience and reduce fraud costs to online businesses.

Though Generative AI (GenAI) has not been around as long as some of the other technologies described herein, customers are keenly aware of its presence, particularly in marketing. Using GenAI wisely can be advantageous, but it should not interfere with what your users want to do on your digital estate. AI-powered chatbots may be helpful in some instances, but they can also be annoying and dissuade users from further interaction.

Deploying modern CIAM, FRIP, GenAI, and privacy protecting solutions properly, with optimizing the customer journey as the primary design principle, will lead to better business and consumer outcomes.



About the Research

The research was carried out among 14,009 general respondents in Australia, Brazil, Canada, France, Germany, India, Mexico, Japan, Netherlands, Singapore, Sweden, United Arab Emirates (UAE), 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.





Contact us

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

cpl.thalesgroup.com/digital-trust-index

