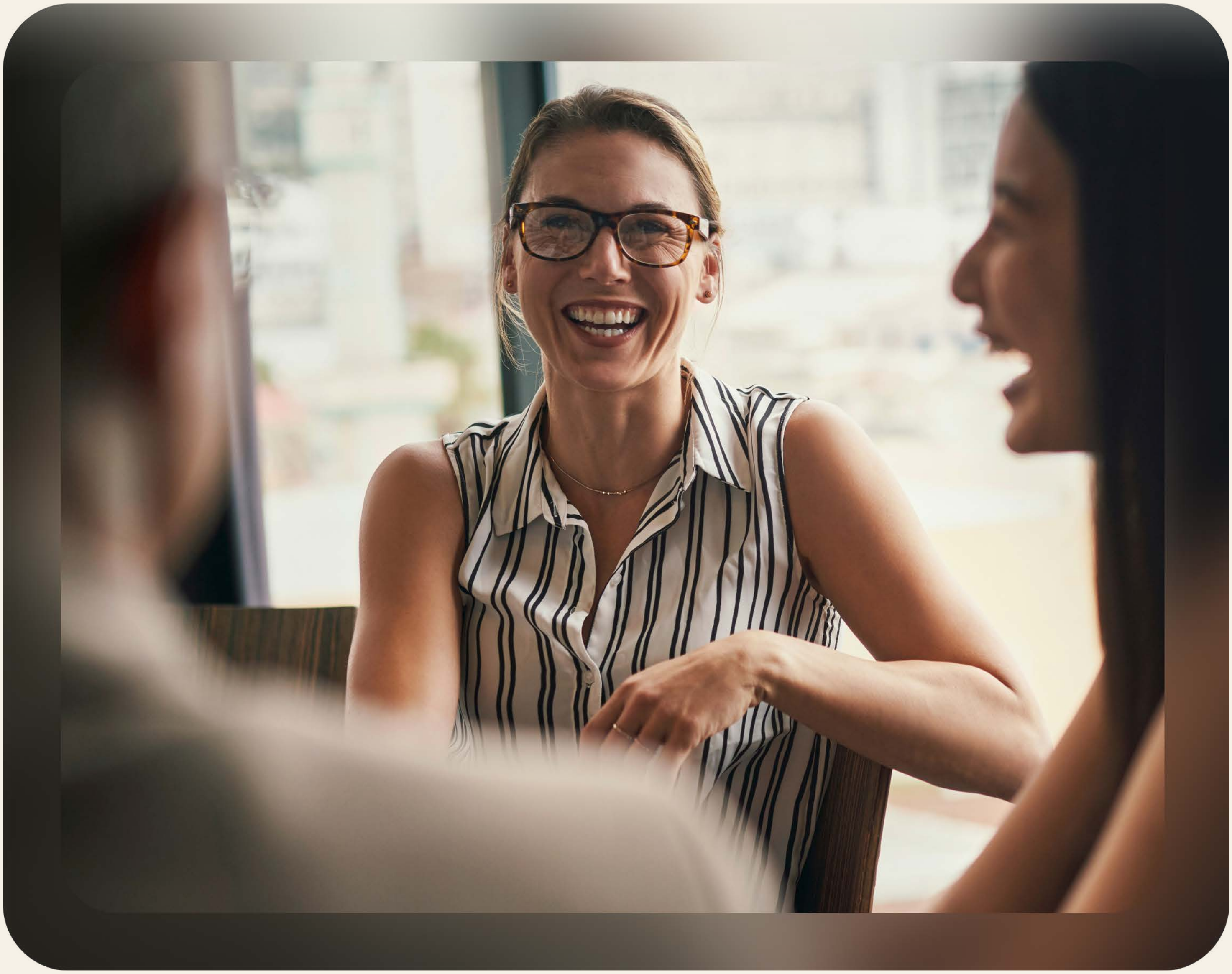
2023

What consumers really want in online experiences

Privacy concerns trump convenience

The hidden costs of passwords

Customer Identity Trends Report



okta

Customer Identity Trends Report

Introduction

It's no secret that delivering a great customer experience boosts revenue and helps brands earn long-term loyalty. But changing consumer expectations and evolving privacy regulations pose new challenges, especially for brands competing in the digital space. So how can marketing and digital leaders respond? We turn to consumers themselves for answers.

Okta commissioned a Statista survey of more than 20,000 consumers in 14 countries, spread across North America (NA), Europe (EUR), and Asia-Pacific and Japan (APJ).[1] In this report, we unpack the results of that survey and examine customer attitudes toward convenience, privacy, and security, and the implications for brands, including:

- Consumer account proliferation and its consequences
- Password fatigue and how it affects conversions
- Data privacy and why it matters now more than ever

We close by outlining a handful of strategies and techniques that organizations can use to answer the paradoxical question that is becoming central to succeeding in the digital marketplace: how to deliver highly personalized experiences without running afoul of customer preferences or regulatory restrictions.

Consumer expectations present new challenges

Let's start with why meeting customer expectations is so challenging right now. There are a few factors at play:

- **Privacy and regulatory concerns demand new solutions:** Consumers are understandably becoming more protective of their private data, but it's these very details that often drive personalized services and offers. Third-party cookies are also disappearing, and some mobile device manufacturers are restricting the use of device identifiers and making it easier for users to opt out of app-specific targeting or tracking.

  At the same time, regulators are imposing strict limits on how data is collected and used. Together, these shifts are forcing many brands to reassess how they gather and use customer intelligence.

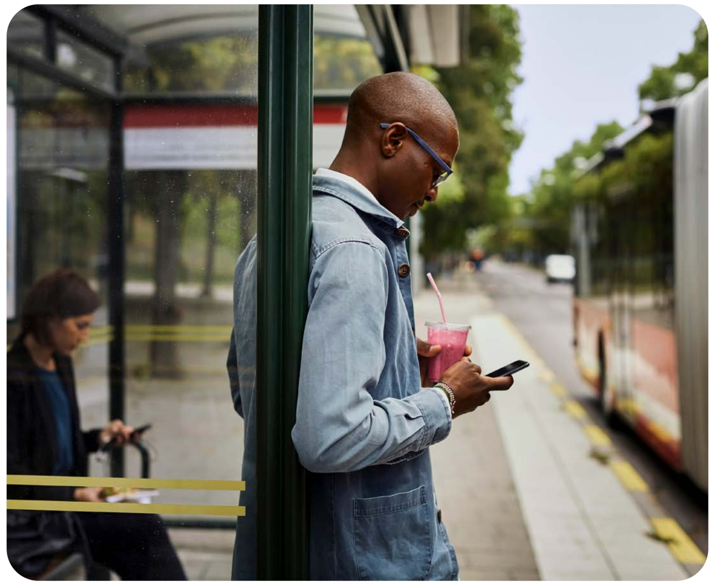
- **Tolerance for information sharing varies widely**: Consumers are inconsistent, adjusting their preferences from industry to industry, and even from brand to brand. What's considered an acceptable information request when setting up a financial account may exceed what's regarded as appropriate for an entertainment experience. Similarly, consumers may be more tolerant of a clumsy experience with a brand they love than with a brand they don't trust.

- **Digital consumers want customization:** Users expect a frictionless, personalized, and instantaneous experience when logging in to an account and engaging with a provider's services — whether that means browsing an online catalog and making a purchase, or booking travel and accommodations, or accessing a healthcare portal.

Salesforce's State of the Connected Customer report reveals that 73% of consumers expect companies to understand their unique needs and expectations (up from 66% in 2020), and 88% of consumers say that the experience a company provides is as important as its product or services (up from 80%).

[1] All conclusions and statistics in this report are based off of the survey unless otherwise noted.

Customer Identity powers customer journeys

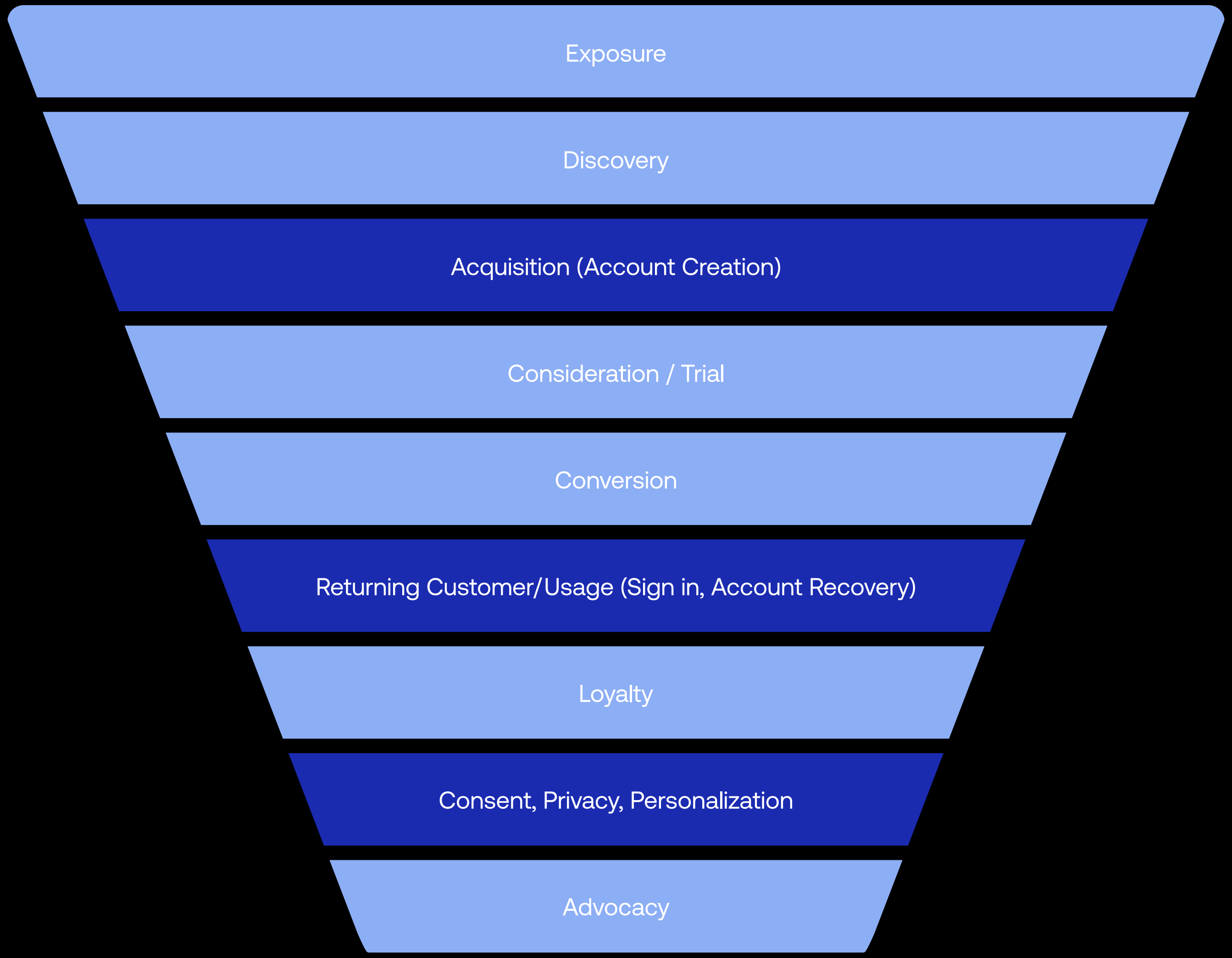


A user's overall experience is hugely dependent on how the Customer Identity journey is managed — from providing seamless single sign-on (SSO) and quick-and-easy multi-factor authentication (MFA), to enabling guest checkouts, or requiring accounts (and asking for customer information).

In fact, Identity flows are fundamental elements of the customer journey (Figure 1) and strongly influence conversion rates. That is why brands in every industry and sector must find the right balance between:

- **User convenience:** Consumers' conscious selections and subconscious preferences both favor convenient experiences, and new experiences are often compared against the most convenient ones
- **Security:** Businesses can be ruined, or at a minimum suffer severe brand and valuation damage from a single breach, so ensuring that their Customer Identity solution meets the highest levels of security is critical
- **Privacy:** To avoid reputational damage and regulatory penalties, businesses must meet ever-changing privacy and compliance requirements

Figure 1: The customer journey heavily depends on Identity flows


Exposure
Discovery
Acquisition (Account Creation)
Consideration / Trial
Conversion
Returning Customer/Usage (Sign in, Account Recovery)
Loyalty
Consent, Privacy, Personalization
Advocacy

Source: Authentication After Passwords

Key Customer Identity terms

Throughout this report, we use a number of subject-specific terms:

- **Account takeover (ATO):** A desired outcome of many attacks against Identity and Access Management (IAM) systems, in which a threat actor gains access to and control over an existing account belonging to a legitimate user
- **Authentication:** How apps identify who users are
- **Authorization:** How apps determine what a user is permitted to do
- **Customer Identity:** How brands continuously learn about their customers and securely build consent-based trust by understanding who their customers are and how they want to engage
- **Customer Identity and Access Management (CIAM):** How companies give their end users access to their digital properties as well as how they govern, collect, analyze, and securely store data for those users
- **Digital footprint:** The trail of data that is left when users interact with digital applications, assets, and services
- **Digital Identity:** The set of attributes that define a particular user in the context of an application
- **Friction:** In the digital world, friction refers to anything that slows down a person's interactions with your service. These interactions may include (but are not limited to) a user: signing up for your service, logging in to their existing account, recovering lost account information, and checking out a purchase.
- **Multi-factor authentication (MFA):** A user verification method that requires more than one type of user validation (e.g., biometric, one-time passcode, or authenticator application)
- **Passwordless:** Passwordless authentication (often shortened to "passwordless") refers to any mechanism that authenticates a user without requiring them to enter their password
- **Single sign-on (SSO):** An authentication solution that permits a user to log in once, with a single Identity, and then access additional independent systems without re-entering authentication factors
- **Social login:** An implementation of single sign-on that allows users to log in to multiple applications and services using a single account, usually from a social networking provider

More accounts. More Problems.

Account proliferation has consequences

Identity insights:

- **Competition for attention and dollars is fierce:** The average online customer has more than 20 active accounts for applications and websites
- **Inactive accounts create Identity risks:** In general, the more accounts a user has, the greater their exposure to data breaches — especially when many of those accounts are forgotten or not maintained
- **Maintaining relevance, particularly with younger generations, is difficult:** Consumers are constantly churning accounts, with younger users doing so at nearly double the rate of older demographics
- **Transparency can help build loyalty:** The large majority of users understand that their online activities leave a data trail, and a large proportion are taking steps to control their digital footprints

As online or click-and-mortar interactions play larger roles in our lives, so too does the number of accounts each of us must manage.

Password managers, browser plugins, and digital wallets can all help to reduce the management burden, but the survey indicates that even with such solutions available, there are limits to how many active accounts the average consumer is willing to maintain — a reality that has potentially significant implications for online brands.

Maintaining relevance is an ongoing challenge

Regardless of their home region, consumers have a similar number of active app or website accounts. In all three regions:

- The median number of active accounts falls in the 10-to-20 range
- The mean is in the mid-20s
- Approximately 75% of respondents have 10 or more active accounts
- At least 35% have 20 or more — led by Europe, with 39%

However, when we look at consumer demographics — particularly age — differences appear. Broadly, younger respondents have a higher number of active accounts, and older respondents have fewer active accounts:

- Respondents aged 18 to 39 years have 26 active accounts, on average, compared to 22 accounts in the 50-to 59 age range and only 20 for those who are 60 or older
- 37% of respondents in the 60+ demographic report having fewer than 10 active accounts, approaching double the proportion (21%) of those aged 18 to 39 who reported the same

In each of the three survey regions, consumers report that they have created an average of three or four new online accounts in the three months preceding the survey, and at least 40% of respondents in each region report creating five or more. The most significant regional discrepancy is that 27% of respondents from Asia-Pacific and Japan report that they have not created any new accounts in that timeframe, a much higher proportion than their peers in North America (19%) and Europe (15%).

Younger cohorts report creating new accounts at a much higher rate than the older cohorts. For example, the 18-to-29 group created more than four new accounts, on average, in the last three months — double that reported by the 60+ group; the other groups fit neatly on a steady gradient between those two extremes.

Because the survey demonstrated very little difference between the average number of accounts in the 18-to-29, 30-to-39, and 40-to-49 age groups, it's reasonable to conclude that these new registrations represent churn (i.e. introducing a new active account by 'retiring' another), rather than net new additions to a user's collection of active accounts. An extension to this interpretation is that the younger a consumer is, the more dynamic their account "library" — and the harder brands have to work to maintain relevance. ■

Estimated number of active accounts, by respondent region

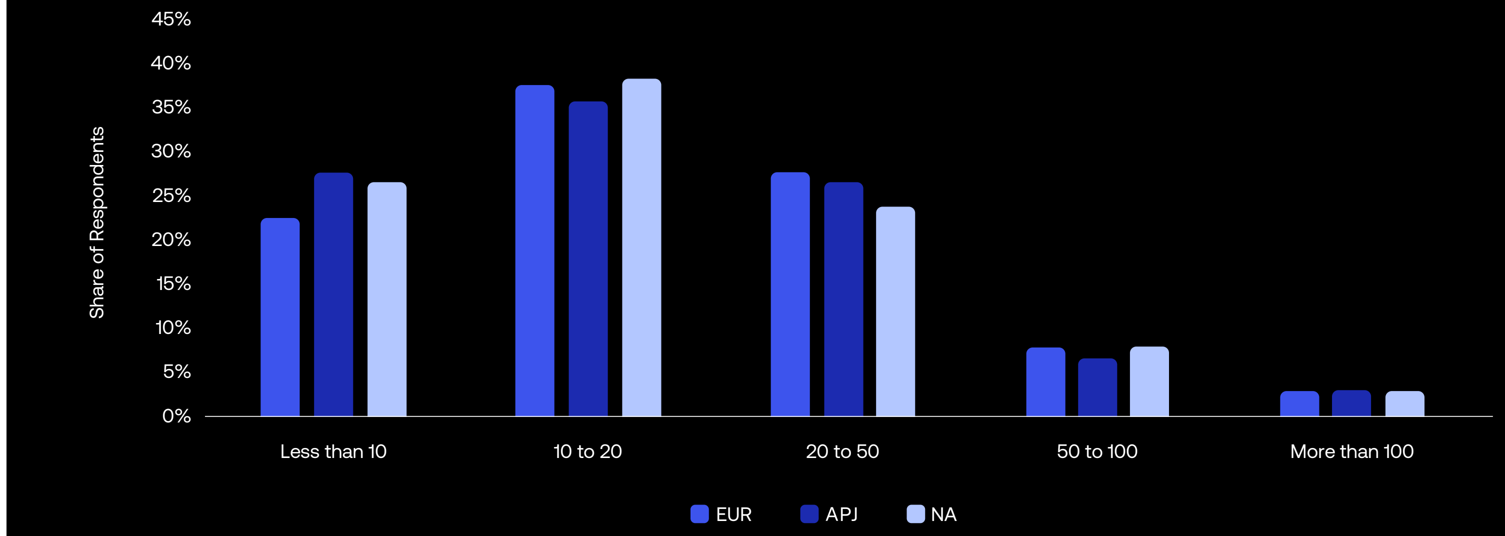


Figure 2: How many active apps and/or websites (e.g., online retailers, banks, insurance agencies, fitness providers, restaurants, etc.) do you have an account with?

Estimated number of active accounts, by respondent age

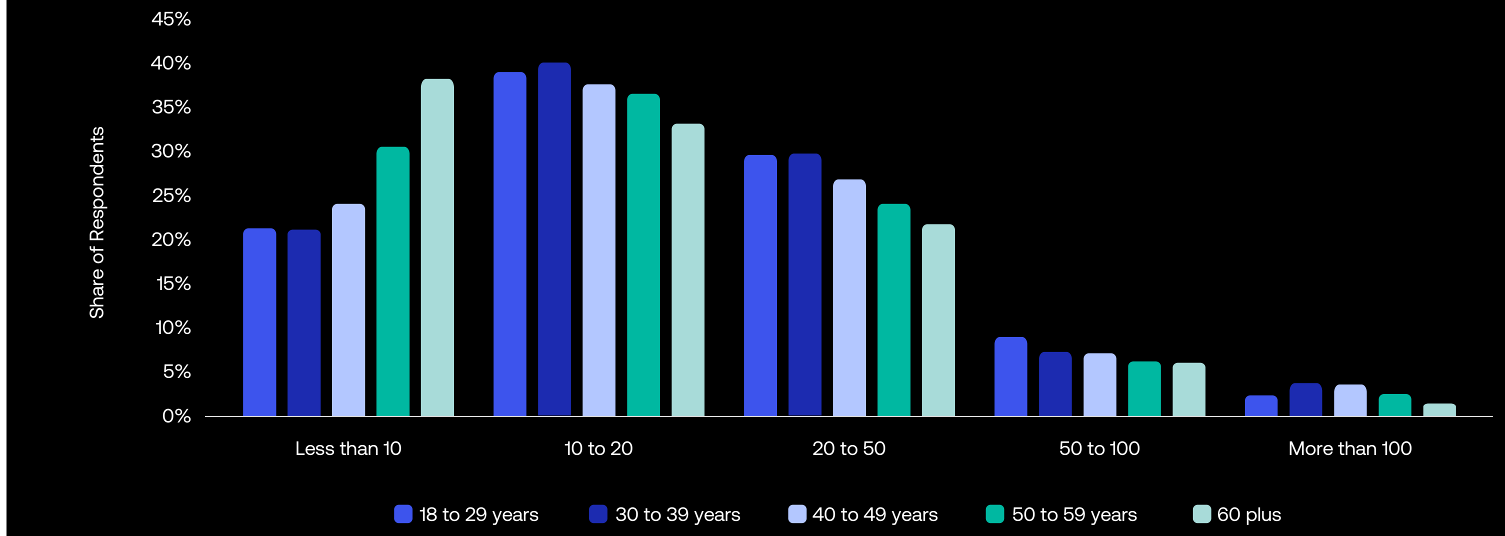
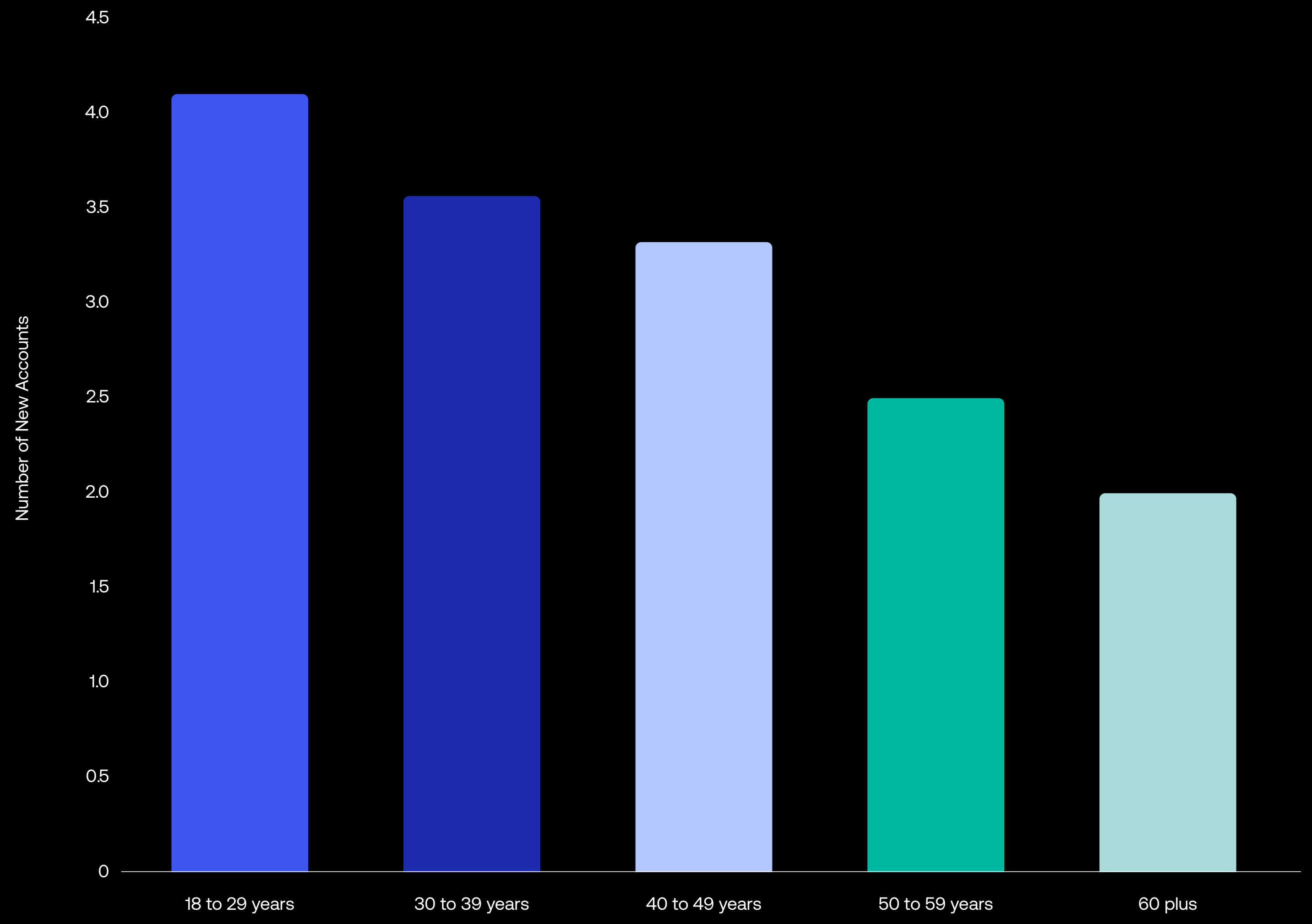


Figure 3: How many active apps and/or websites (e.g., online retailers, banks, insurance agencies, fitness providers, restaurants, etc.) do you have an account with?



Estimated number of new accounts registered, by respondent age

Figure 4: How many new online accounts have you registered for in the last three months?

Customers are trying to manage their digital footprints

The survey revealed that the large majority — about 71% — of respondents are aware that their online activities leave a data trail; moreover, the larger proportion of that group (about 62%, or 44% of respondents overall) report that they try to take steps to mitigate it.

Notably, this general point holds true regardless of consumer region, age, and gender (although men had a higher rate of applying mitigating measures).

Given the strong competition for customer attention, this finding suggests that brands that want to build long-term customer loyalty should be transparent about what data is needed and how it's used to power a private, secure, and convenient experience, and should provide customers with tools to manage their preferences.

In addition to being consistent across regions, these results showed little variation across age cohorts. While older groups have significantly fewer accounts than younger generations, they're just as aware that their online activities leave traces in the digital world.

Inactive accounts create Identity risks

Note that the survey question behind Figure 2 focused only on "active" accounts, and it's reasonable to conclude that the total number of accounts each respondent has is higher — perhaps considerably so.

This long trail of digital footprints has potentially serious consequences, both for user privacy and for the security of their other accounts.

In general, the more accounts a user has, the greater their exposure to data breaches — especially when many of those accounts are forgotten or otherwise not maintained (a consequence of the aforementioned account churn). A breach to any one of these services may equip a threat actor with a huge volume of user credentials and associated personal data.

Cybercriminals are adept at using this information at scale to compromise accounts that consumers have with other brands. In fact, over 80% of breaches involving attacks against web applications can be attributed to stolen credentials, according to Verizon's 2022 Data Breach Investigations Report.

In other words, a customer's active account with your service may be at risk of account takeover due to an account they haven't used or even thought about in years — especially if that customer reuses (or only slightly alters) passwords, or if your password recovery functions only rely on security questions. ■

If you use a password manager or other system to manage account credentials, try this exercise:

- Take a guess as to how many accounts you have.
- Next, open the password manager and see how many websites and apps are stored within it.

Does the answer surprise you? Odds are that the longer you've had the system in place, the more surprised you may be.

Want to learn more about how threat actors can target your customers and what you can do to stop them?

Check out Auth0's State of Secure Identity report.

Top five countries, by proportion of respondents who are aware of their digital footprint:

Italy	85%
Spain	83%
Germany	81%
Netherlands	79%
Sweden	79%

Top five countries, by proportion of respondents who try to manage their digital footprint:

Spain	59%
Italy	55%
Germany	50%
France	50%
United States	48%

The costs of friction

Passwords belong in the past

Identity insights:

- **Friction is the enemy of conversions:** A significant majority of survey respondents indicated that they would be more likely to spend money when services offered a simple, secure, and frictionless login process
- **Passwords are a major source of frustration and lost business:** Faced with cumbersome requirements and frequent problems logging in, many users simply abandon accounts
- **Passwordless options offer an opportunity:** Almost two-thirds of survey respondents report feeling overwhelmed with the number of usernames and passwords they have to manage

In the near future, traditional login will become extinct. Today's login boxes, with their ubiquitous user ID and password fields, will be replaced by user-centric systems that favor convenience (without sacrificing security or privacy) and are built on trust.

This shift will benefit consumers and service providers alike by reducing customer frustration and removing barriers that can impede digital transactions.

Less friction means more revenue

For consumer businesses, friction is a major obstacle to conversions and, by extension, to revenue. In fact, nearly 60% of survey respondents indicated that they would be more likely to spend money when services offered a simple, secure, and frictionless login process. This finding is consistent across all sectors/industries, suggesting that users crave convenience in every interaction.

While there were some regional differences, age groups show the largest variation: Younger consumers are about a third more likely than older consumers to spend more money when offered a great login experience.

While some amount of friction is necessary to establish trust and provide security controls, lowering friction wherever practical — in any and every consumer interaction — can increase conversion rates and, accordingly, grow revenue in both the short and long term. ■

Share of respondents likely to spend more with simple, secure, and frictionless login, by respondent region

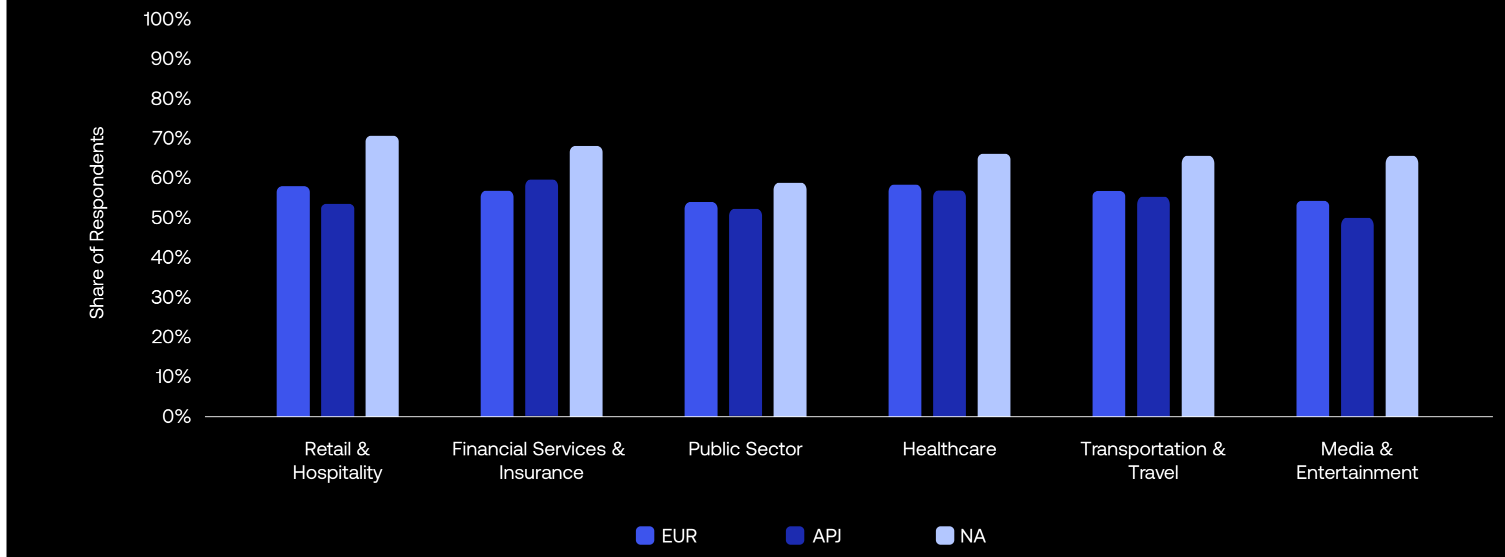


Figure 5: When interacting with a brand online, would you say you are more or less likely to spend money if you know the login process is simple, secure, and frictionless? The graphs show the sum of "Very likely" and "Somewhat likely" responses.

Share of respondents likely to spend more with simple, secure, and frictionless login, by respondent age

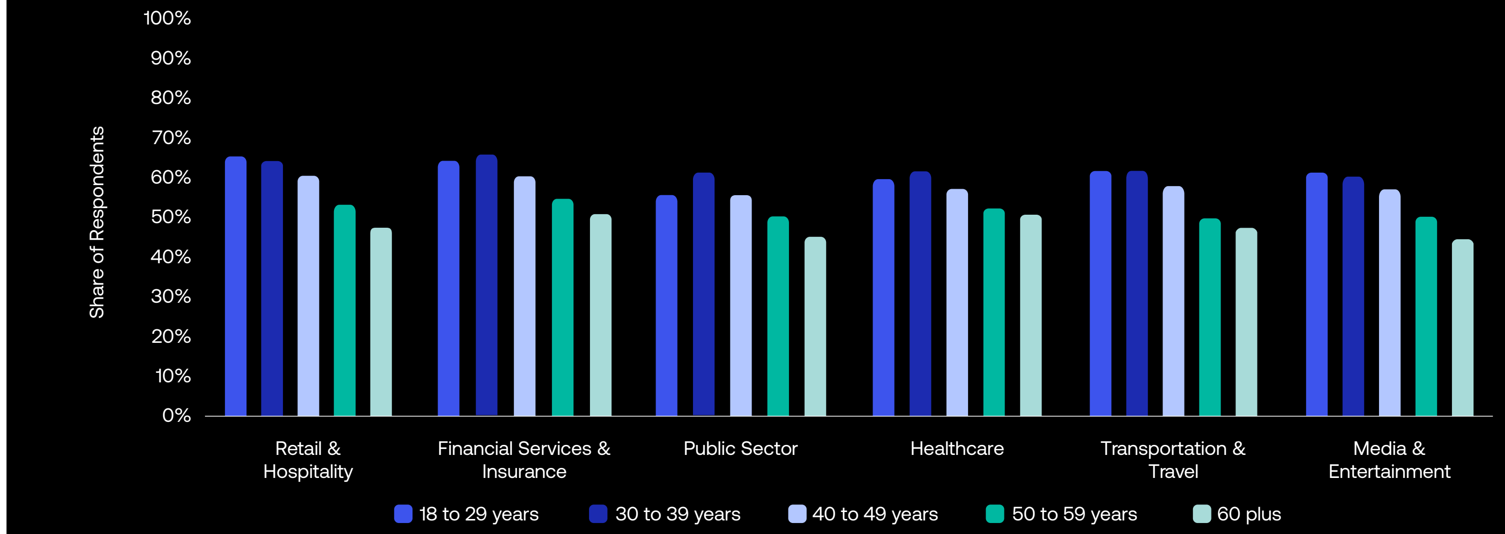


Figure 6: When interacting with a brand online, would you say you are more or less likely to spend money if you know the login process is simple, secure, and frictionless? The graphs show the sum of "Very likely" and "Somewhat likely" responses.

Passwords cause problems

Perhaps nothing contributes more to friction than passwords, and the frustration begins the moment a prospective customer signs up for an account:

- 33% of respondents indicated feeling frustrated when they have to create a password that meets certain requirements
- 25% reported frustration with needing to create a new password for every online service

Notably, customers are especially intolerant of password creation when signing up for Retail & Hospitality services, suggesting that cumbersome password processes could be a major contributor to cart abandonment.

According to research by Auth0, 83% of consumers have abandoned their cart or sign-up attempt because the login process was too complicated. Often the culprit is a long-forgotten password.

How common is it for consumers to forget login information? The survey says ... very:

- 63% of respondents report that at least once a month they're unable to log in to an account because they forgot their username or password
- 24% encounter this issue at least once a week
- For 6%, it's a daily occurrence

And while resetting a password is usually possible, consumers might decide that the process is simply not worth the effort, leading not only to lost conversions, but also lost users: Only 52% of respondents reported that they still have access to all of their accounts. ■

Use of password managers is consistent across regions, but drops off slightly in older cohorts:

18%	18 to 29 years
17%	30 to 39 years
18%	40 to 49 years
15%	50 to 59 years
13%	60 plus

Going passwordless pays

Once you recognize the dangers of friction and how it manifests, it follows that:

- Identity flows (such as account creation, sign in, and consent) are fundamental parts of the customer journey
- Friction can mean the difference between making or missing your conversion (and revenue) goals

Viewed through this lens, the cost of friction within Identity flows becomes clearer. For example, consider the average lifetime revenue associated with your business: that's the potential cost of an abandoned account creation. Next, think of the average transaction size: that could be the cost of a failed login attempt.

Fortunately, there are passwordless options that offer both stronger authentication and more convenience for consumers. For example, enabling users to authenticate using their device biometrics has two benefits:

- It reduces friction during authentication, boosting user retention and revenue
- It increases security since the flow is generally not "phishable" by bad actors

In the last few years, the FIDO Alliance, an open industry association formed to reduce reliance on passwords, has been working to help users authenticate with maximum security and minimum friction. The resulting WebAuthn standard provides the foundation for that to happen by allowing brands to authenticate users with public key cryptography instead of a password.

Ready to go passwordless?
Learn how to get started.

With 65% of survey respondents feeling overwhelmed with the number of usernames and passwords they have to manage, odds are strong that a large portion of your customer base and target market will appreciate a more convenient — and more secure — alternative.

Moving toward secure, passwordless options improves the customer experience — and that benefits the bottom line: "By 2025, organizations adopting customer identity and access management (CIAM) with converged fraud detection and passwordless authentication will be able to reduce customer churn by more than half," according to Gartner® research.[2] ■

The accessibility imperative

While friction is an inconvenience for many consumers, it can prevent others from accessing your services.

Consider disabilities like vision or cognitive impairment, or limited motor function, and imagine trying to navigate a cumbersome authentication flow that requires the user to remember and then enter a long, complex password. Or give thought to how a user uncomfortable or unfamiliar with technology would respond to a message asking them to download an app and configure push notifications.

Not only is there a moral obligation to consider accessibility when mapping the customer journey, there is also a considerable financial incentive — by creating experiences for everyone, brands can maximize their market reach.

[2] Gartner®, "Innovation Insight for Customer Identity and Access Management," December 9, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Control trumps convenience

Data privacy matters to today's consumers

Identity insights:

- **Customers want control:** In every region, and across every industry, the large majority of survey respondents want control over what data is collected and how it is used.
- **Control trumps convenience:** Consumers are willing to sacrifice convenience for greater control over their own data; younger cohorts are more receptive to relinquishing some control for a frictionless experience.
- **Passwords prove hard to shake:** Despite the security risks and inconvenience, passwords persist as the most popular authentication measure. However, the tide is turning as younger cohorts adopt new methods, such as biometrics.

For a Customer Identity solution to be effective, it must be secure and easy for consumers to navigate. But finding the right balance between these two can be a challenge: Some amount of friction is necessary both to establish trust and to provide necessary security controls that protect a user's sensitive information and combat fraud, but — as we saw in the previous section — too much friction can have negative consequences.

The threats facing any particular application or service vary enormously by geography, industry, and brand prominence, among other factors. At the same time, different organizations have different risk appetites and exposures. The appropriate level of friction for security measures will vary on a company-to-company basis, and brands should take note that customers are paying attention: The survey found that 75% of global consumers recognize that companies/websites have different security postures in place and understand that some brands will protect their data more than others.

Customers want control over their own data

The large majority of survey respondents, with consistent attitudes across different age cohorts, consider it important to have control over their own data when interacting with a brand online. This view is especially true for Financial Services & Insurance (86% of participants rated control as "very important" or "somewhat important"), Healthcare (83%), and the Public Sector (81%) — all of which are likely to involve sensitive or private personal information.

In every industry — by anywhere from 6 to 13 percentage points — respondents from North America showed that they value control even more than their European peers, who in turn slightly edged out consumers from Asia-Pacific and Japan.

Across the three survey regions anywhere from 60% (Asia-Pacific and Japan) to 73% (North America) of respondents are aware of their own security practices; about a third of those users are employing a range of tactics to protect their own data, with the most common being:

- Using strong passwords (cited by 60% of respondents who are taking steps to protect their own data)
- Restricting the data they share (46%)
- Regularly deleting cookies (43%)
- Using different passwords for each account (42%)
- Regularly reviewing/changing privacy settings (29%) ■

Share of respondents indicating control is important, by respondent region

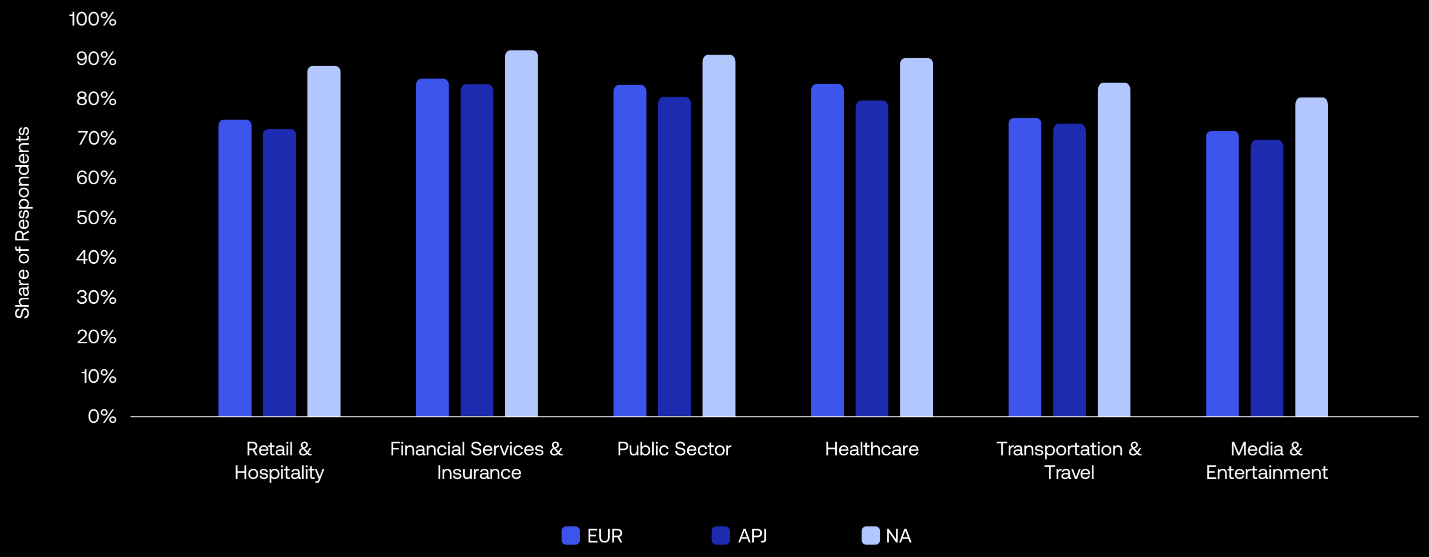


Figure 7: When interacting with a brand online, how important is it to you to have control over your data (e.g., change the privacy settings, limit the information you have to share)? The graphs show the sum of "Very important" and "Somewhat important" responses.

Share of respondents indicating control is important, by respondent age

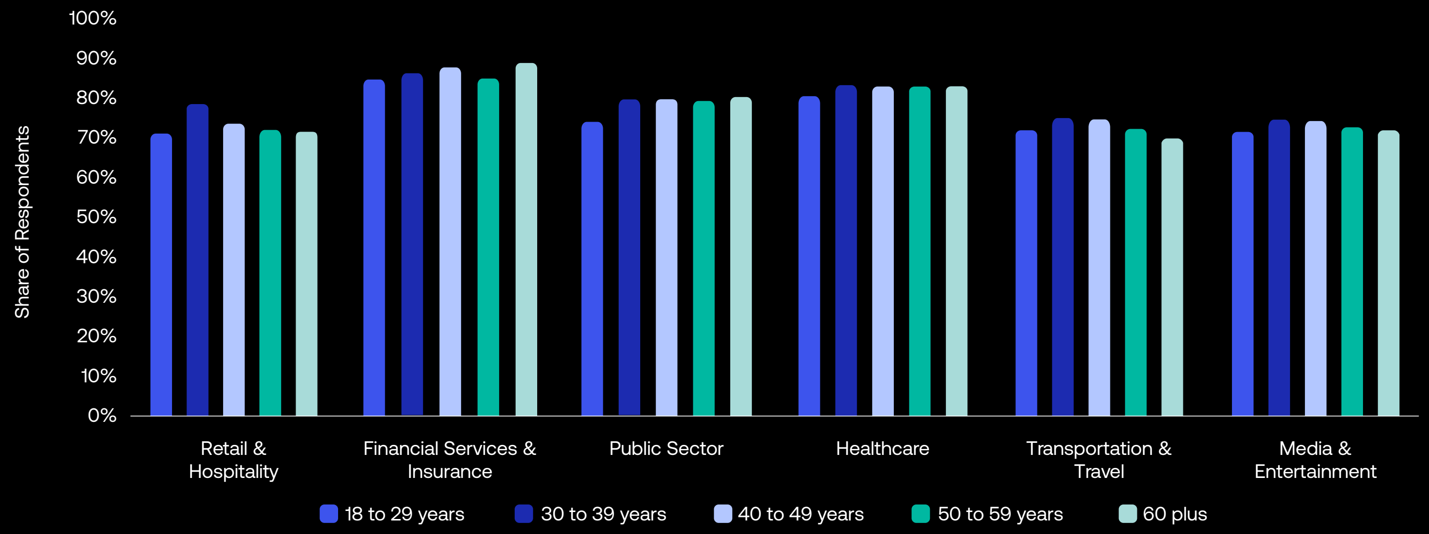


Figure 8: When interacting with a brand online, how important is it to you to have control over your data (e.g., change the privacy settings, limit the information you have to share)? The graphs show the sum of "Very important" and "Somewhat important" responses.

Customers value control even more than they value convenience

In fact, control matters so much to today's consumers that, when forced to choose between compromising control for convenience or vice versa, respondents favored maintaining control — especially when engaging with Financial Services & Insurance, Healthcare, and the Public Sector.

Notably, the matter of control versus convenience exhibits considerable variation by region and age.

For instance, respondents from Europe and North America favored control across every industry; in Asia-Pacific and Japan, though, users were willing to compromise control for a lower-friction experience when interacting with brands in Media & Entertainment, Transportation & Travel, and Retail & Hospitality.

We also see clear correlation between age and attitudes towards control and convenience: The older the respondent, the stronger their preference to retain control. ■

Respondents preferences for convenience (left) versus control (right), by region and industry

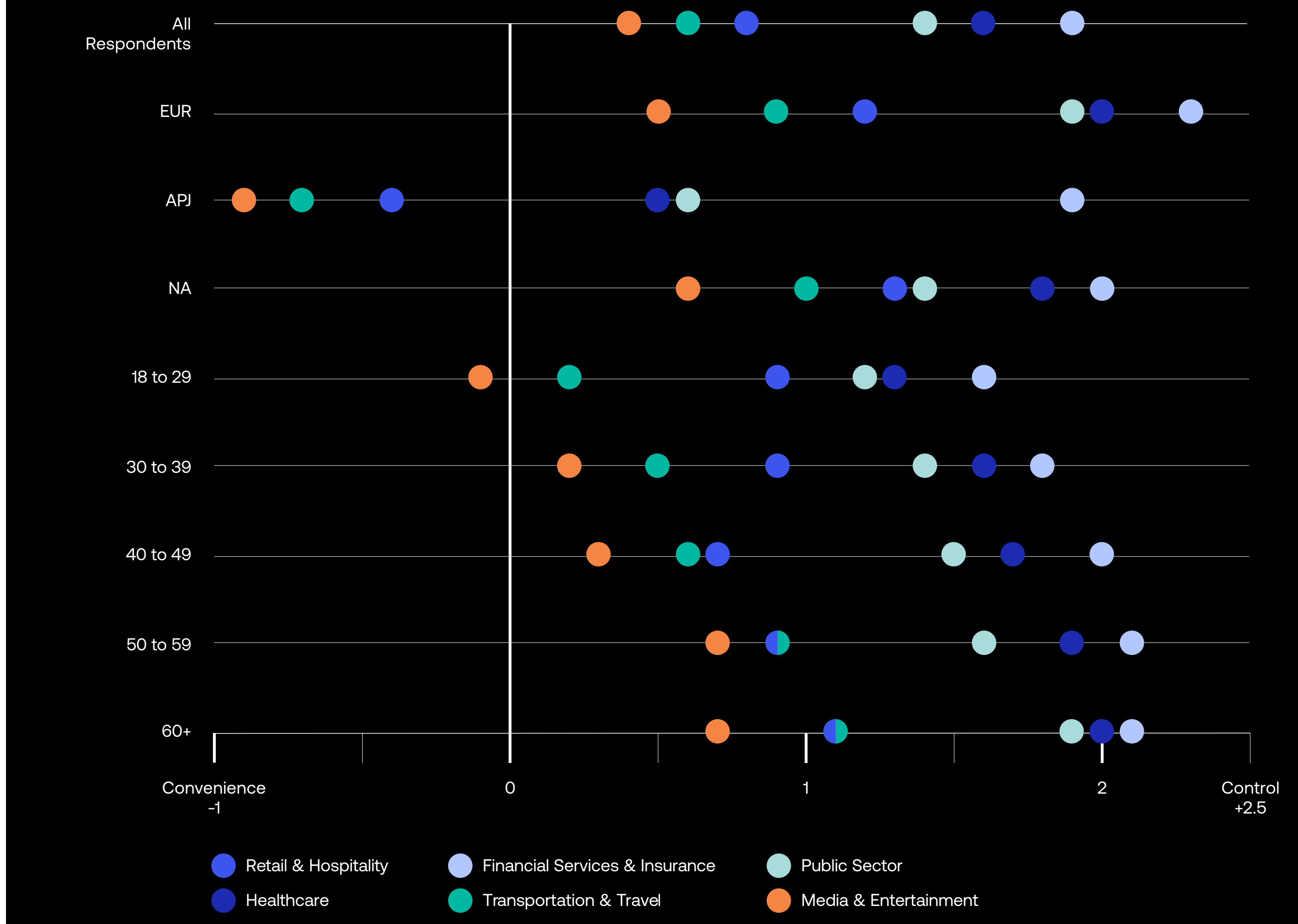


Figure 9: Composite score based on respondents' preferences for a frictionless user experience versus maintaining control over their data. Positive numbers indicate a preference for control; negative numbers indicate a preference for convenience.

Passwords might be hard to manage, but they're harder to shake

While passwords are inconvenient, they're also familiar. Most of us know the drill and expect to create one for new accounts. In this case, familiarity breeds acceptance, and consumers ranked the traditional username-and-password combination highest when asked which authentication methods they considered secure and convenient (they were free to choose multiple options). Passwords led the way across most industries and were especially favored for transactions in Retail & Hospitality, Transportation & Travel, and Media & Entertainment.

On the other end of the preference spectrum, we find social login. With this method, consumers use information from a social network provider like Facebook, Twitter, or Google, to sign in to a third-party website, rather than creating a new account. The value proposition is often convenience – it's one less account to create and remember. This points to security as the limiting factor and suggests that consumers tend to view social login as less secure than other methods. It finds the most support for transactions in Retail & Hospitality and Media & Entertainment, both industries that typically deal with less sensitive information than, say, finance or healthcare.

The data also suggests that some consumers don't find passwords particularly secure. This is especially true for transactions in Financial Services & Insurance. For these, respondents preferred multi-factor authentication (MFA), followed by biometric authentication, both methods that tend to offer a higher level of assurance and phishing resistance than usernames and passwords.

But organizations should note that because of the widespread adoption of MFA, threat actors are increasingly targeting this form of authentication. As attackers become more sophisticated, it's critical that brands implement MFA correctly and use strong secondary factors.

Overall, biometric authentication lagged behind usernames and passwords. Considering its tremendous strength as a security layer, this suggests that biometrics are not well understood by the general population.

MFA is essential to keeping customers secure. Get it right with Okta's Multi-factor Authentication Deployment Guide.

Examining authentication preferences by age shows some very clear divergences. The older the respondent, the more likely they are to prefer the username-and-password combination, and the less likely they are to prefer social login. Although not as pronounced, we see the same trend for MFA, with older cohorts preferring it over their younger counterparts.

Notably, the youngest cohort, those between 18 to 29 years old, has the highest approval for biometric authentication (42%), suggesting that brands would do well to start exploring this method now, especially as this group gains purchasing power. The youngest respondents (29%) also favored social login over the oldest cohort (8%) by a margin of 21 percentage points, indicating that the security measure stands to gain traction in the coming years. ■

Preferred security measure, by industry

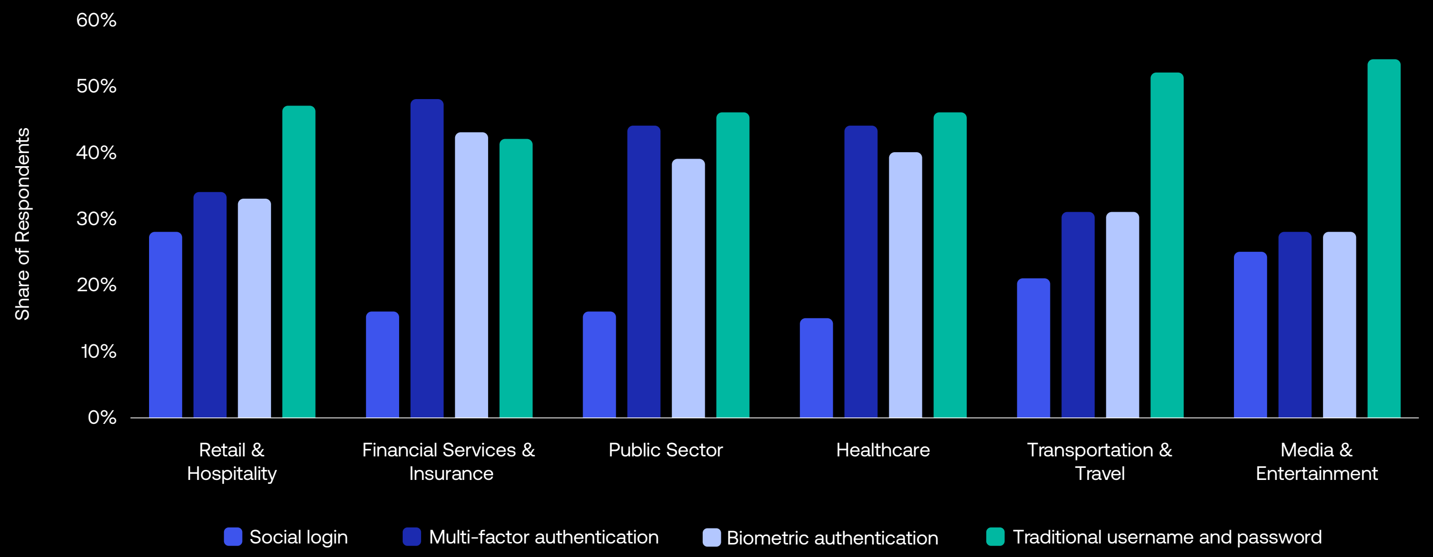


Figure 10: When interacting with a brand online, which of the following security measures do you consider most appropriate based on convenience and security?

Preferred security measure, by age

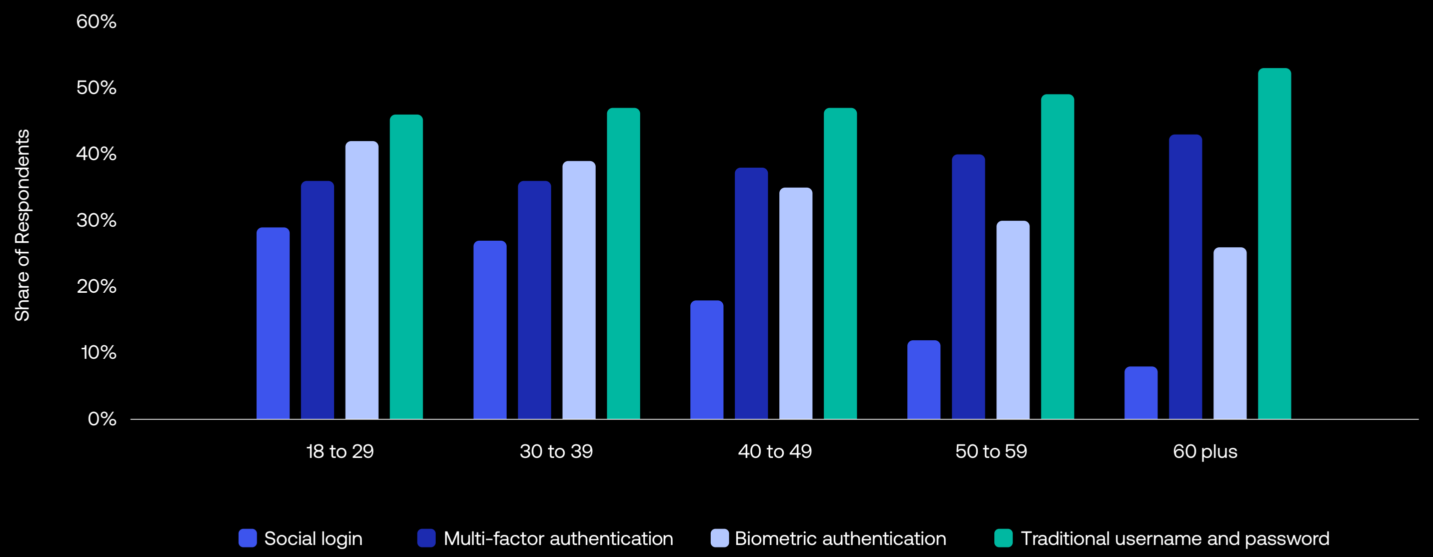


Figure 11: When interacting with a brand online, which of the following security measures do you consider most appropriate based on convenience and security?

Overcoming the privacy-personalization paradox

Considered as a whole, the results of the survey point to a paradox at the heart of online interactions and the digital Identities that enable them: Customers want frictionless, personalized, and instantaneous experiences when logging in to apps and making purchases; at the same time, they want to control what data they share, and they want appropriate security controls in place to protect it.

Complicating matters for brands, a range of factors — including regions, industries, and user demographics — influence preferences and impose specific requirements.

Instead of a singular approach to Customer Identity and Access Management (CIAM), organizations can employ a combination of techniques to meet the personalization, privacy, and security needs of digital consumers.

For example, digital relationships are formed and will progress in the same way relationships do in real life: over time. The burden of establishing trust in a digital relationship will be on the service provider, and this trust must always be earned, respected, and protected.

As Will Grobel, a director with Deloitte Digital describes the situation, "Collecting more first-party data should be a key priority, however this must be done with consideration. Ultimately, as brands' reliance on cookies decreases, consumer trust should increase. For too long, indiscriminate targeting has been prioritized over creating more genuinely personalized experiences."

To reduce friction, built trust, and acquire the first-party data key to personalization, brands must start exploring new solutions, such as:

- **Anonymous checkout** (also referred to as guest checkout), which allows a user to use a service without creating an account; billing and delivery information are collected to facilitate the transaction, but are not stored within an account
- **Progressive profiling**, which gradually asks the user for information (and introduces them to new authentication options) as they experience more value from the service — while still allowing them to get started very quickly

Similarly, by moving away from the traditional username-and-password combination, brands can concurrently strengthen security and create more convenient user experiences. Again, a number of techniques are available to achieve the optimal balance appropriate to different scenarios:

- **Social logins** streamline account authentication and reduce the risk that users will encounter problems when trying to log in to your services
- **Biometric authentication** dually achieves convenience and security and is increasingly supported by consumer devices
- **Adaptive MFA** is a tool that only engages secondary factors when a user interaction is deemed risky based on behavioral data (e.g., an impossible travel scenario or a login from a new device)
- **Step-up authentication** adapts Identity requests to the importance of the resources being accessed (e.g., a user may be prompted for additional authentication when attempting to alter account information or retrieve a sensitive document)

Finally, organizations can be transparent with users about how digital Identities are managed, including why data is needed and how it will be used, and what security measures are in place to protect user accounts and the private data within them.

> "With digital transformation and pressure to build orchestrated Identity into the customer journey, CIAM solutions are an essential building block of customer management."
>
> The Forrester Tech Tide™: Identity And Access Management (IAM), Q1 2023

Methodology

Commissioned by Okta, Statista conducted a global survey of 21,512 consumers from 14 countries: the United Kingdom, Germany, France, the Netherlands, Sweden, Ireland, Spain, Italy, Switzerland, the United States, Canada, Australia, Japan, and South Korea.

We refer to this survey as "our survey" and "survey" throughout, and refer to the people who completed the survey as "survey respondents" or "respondents."

Data was collected in August 2022 and February 2023 using an email invitation and an online survey. All participants were at least 18 years old.

Region	Country	Respondents	Share
Europe (EUR)	United Kingdom	2,000	9.3%
	Germany	2,000	9.3%
	France	1,500	7.0%
	Netherlands	1,500	7.0%
	Sweden	1,000	4.6%
	Ireland	1,000	4.6%
	Spain	1,000	4.6%
	Italy	1,000	4.6%
	Switzerland	1,000	4.6%
North America (NA)	United States	3,000	13.9%
	Canada	1,502	7.0%
Asia-Pacific & Japan (APJ)	Australia	1,501	7.0%
	Japan	2,004	9.3%
	South Korea	1,505	7.0%
	Total	**21,512**	**100%**

Gender	Respondents	Share
Male	10,613	49.3%
Female	10,789	50.2%
Other	74	0.3%
Prefer not to say	36	0.2%

Age Cohort	Respondents	Share
18 – 29 years	5,012	23.3%
30 – 39 years	5,040	23.4%
40 – 49 years	4,886	22.7%
50 – 59 years	4,595	21.4%
60+ years	1,979	9.2%

About Okta

Okta is the world's Identity company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.

Disclaimer

This document and any recommendations about your security practices are not legal, security, or business advice. This document is intended for general informational purposes only and may not reflect the most current security and legal developments nor all relevant security or legal issues. You are responsible for obtaining legal, security, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of the recommendations in this document.

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871