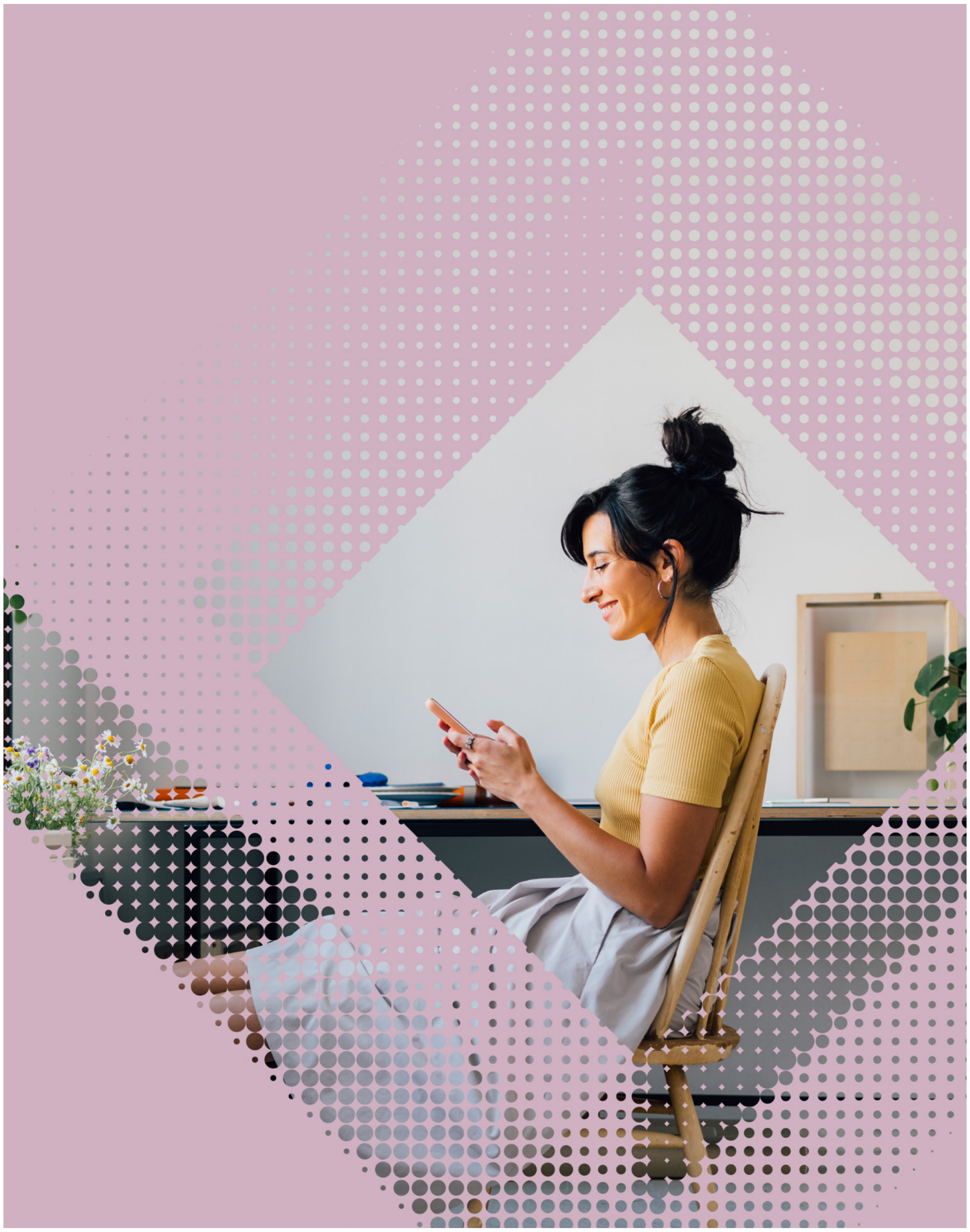
Whitepaper

September 2022

Why Your Customers Aren’t Converting:

A Global Study on the Role of Customer Identity and UX

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



okta

Contents

Executive summary

A polished user experience (UX) is the foundation for every sustainable, profitable digital business.

Chief Marketing Officers (CMOs) and Chief Digital Officers (CDOs) know that streamlined digital experiences directly translate to revenue. Clunky navigation and long page load times aren't purely technical issues. They drive user attrition and reduce the likelihood of a successful conversion.

And that's not all. Identity, or how people prove who they are when accessing digital services, is another key point of conversion weakness. It's a missed opportunity for marketing leaders to do better and to have a bigger impact on the business.

We set out to discover more. A recent analysis into survey data we conducted with global market research firm YouGov reveals two strategic areas of opportunity for marketing and digital leaders—widespread issues of cart abandonment caused by unwieldy login and account creation flows, and the sluggish adoption of advanced identity technologies customers love and want.

For example, we found that:

58% Of marketing leaders, whose businesses require consumers to login/sign-up to use their services, believed their sign-up processes led to a higher likelihood of cart abandonment, a finding echoed by the very consumers they are trying to engage.

63% Did not utilize social login, an increasingly popular alternative to traditional sign-ups. Here users can sign into an app or webpage via their social media credentials such as Facebook or Google. It may seem minor, but offering alternatives to the traditional username/password combo can increase conversion rates and lower friction, among other benefits.

You'll also learn about the adoption rates of customer identity solutions in consumer-facing applications, how your sign-up times may stack up to your competitors, and why it's a big myth that UX friction is a necessary cost of security.

Methodology

The survey was conducted between February and August 2021 by Auth0 (now Okta Customer Identity Cloud) with YouGov. A further analysis of specific marketing responses was done in September 2022. The full report consists of two surveys with more than 16,700 consumers and more than 2,800 IT and marketing decision makers. The sample referenced here includes 908 senior marketing and digital decision makers working for companies that offer services/applications to consumers. The full set of respondents were based in 14 countries: US, UK, Belgium, France, Germany, the Netherlands, Australia, Singapore, Japan, Argentina, Brazil, Mexico, Chile, and Finland. For this report, CMO's and CDO's are referred to as 'Marketing leaders'.

Introduction

According to the 2022 Salesforce State of the Connected Consumer report, 88% of consumers said the experience provided by a company is of equal importance to the product or service. The market rewards companies that prioritize UX too. According to one study, every dollar invested in UX returns $100. That's an ROI of 9,900%.

Still, crafting an elegant UX isn't easy. Blind spots do exist within your digital teams. They often tolerate friction in the name of security. But here's the thing: friction isn't a prerequisite for a robust identity system. Businesses can enjoy the best of both worlds: something that smooths the path between initial sign-up and a sale, while also ensuring maximum security.

Key takeaways

Our survey tackled several core topics:

- **The cost of bad identity UX.** Your would-be customers are paying attention to your sign-up processes and many land somewhere between underwhelmed and flat-out frustrated. It's no secret—56% of marketing leaders described their sign-up processes as a "likely factor" behind cart abandonment.

- **Safety first.** Consumers worldwide want to transact with organizations that take their security seriously yet your digital teams aren't making it easy to evaluate the safety of an app or site. In our wider survey, fully half of all Japanese consumers—50%—found it difficult to identify apps and online services that will keep their personal information safe.

- **The identity feature gap.** Advanced identity features are popular among security savvy consumers, but not all marketing leaders report taking advantage of them. Just 37% of marketing leaders surveyed reported offering one advanced option—social login—to their customers.

Let's dive into each.

The cost of bad identity UX

In our analysis, the CMOs and CDOs we surveyed overwhelmingly blamed their identity UX for their cart abandonment rates.

Respondents were more likely than not to be critical of their sign-up processes, with 56% describing them as a “likely factor” behind cart abandonment. Just 24% of those surveyed did not believe their sign-up processes affected conversions.

Of the sample of marketing leaders, 20% believed their sign-up flows were “extremely likely” to influence cart abandonment, while 36% said they were “somewhat likely.”

Login flows for returning users fared slightly better. Nearly half of marketing leaders surveyed—46%—described it as a “likely” factor behind cart abandonment, compared to 33% who said they were an “unlikely” influence.

The causes of cart abandonment are varied. The Baymard Institute’s long-running survey of American consumers illustrates this well and agrees identity UX plays a huge role. The second-most commonly cited reason behind cart abandonment is the need to make an account for an online retailer. This frustration was only surpassed by unexpected fees (like shipping and tax), which took the top spot.

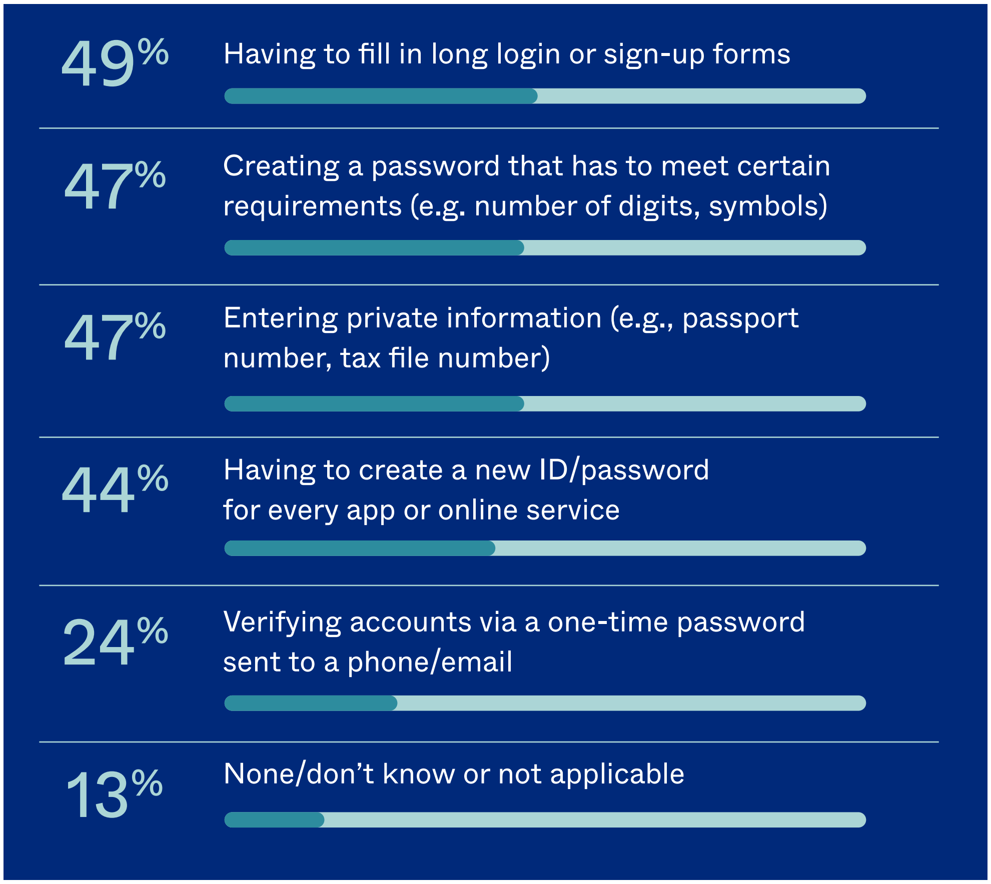
Time is also a factor. Half of marketing leaders surveyed—48%—estimate it takes consumers more than a minute to register a new account. From the total sample, 24% estimated their average sign-up times as between one and three minutes.

At the higher end, 4% claimed their sign-up processes take over 10 minutes to complete. Ten minutes!

Obviously, the time it takes to create an account is influenced by a number of factors. Fintech and gaming products, for example, require know-your-customer (KYC) information. This takes time for the customer to provide and for the platform to verify. You can’t eliminate every piece of friction your customer will face. But with help you can limit it until only the most essential elements remain.

Lastly, global marketing and digital leaders take note: Consumers in Asia-Pacific and Latin America were more likely than those in EMEA and the US to find having to fill in long login or sign-up forms frustrating (APAC 55% and LATAM 52% compared to EMEA 46% and the US 36%).

Today’s consumers express these top frustrations:



Safety first

Your potential customers are eager to identify and transact with apps and online services that will keep their personal information safe.

Are you and your teams making this easy or difficult?

Looking globally across our full sample, Japanese (50%) and German (48%) consumers were more likely than those in all other markets surveyed to say they find it difficult to identify apps and online services that will keep their personal information safe. Overall, less than 3 in 10 (28%) found these offerings easy to identify.

We will get deeper into solutions in a bit, but biometrics are definitely one area to watch when it comes to signaling a commitment to security.

When asked about biometrics— a cybersecurity process that verifies a user’s identity using their unique biological characteristics, such as fingerprints, voice, or face, as their password,—44% of consumers said they are more likely to sign up to an app/online service if a company offers biometric authentication.

Knowing your customer starts with login

Your customers' experience with your digital brand begins when they first visit your site and is solidified with their first visit to your primary point of customer interaction—the login box. No other aspect of your web presence is as pervasive in the lives of your customers, since they have to login before beginning every other interaction with your brand.

So doing customer identity well is all about striking the right balance of factors for that contact point. Your visitors expect a frictionless experience while having privacy concerns for the personal information they're sharing with you. At the same time, you need to know that this public-facing access point is secure from intrusion by bad actors. It's in this mix of security, privacy, and customer experience (CX) that you will be able to capture, convert, and retain those customers.

The identity feature gap

There are the identity features you are offering and the identity features your customers want.

If there is a gap, it's worth addressing.

Social login and biometrics join adaptive multi-factor authentication (MFA), single sign-on (SSO) and passwordless options as features that have demonstrable identity and security benefits. But, as the results of our survey demonstrate, many digital businesses fail to implement them and realize their advantages.

Here's what we found:

37%	Of marketing leaders surveyed reported offering social login to their customers.
26%	Have adopted biometric authentication
21%	Reported using passwordless authentication
30%	Say their companies' apps use multifactor authentication

Each of these technologies has the benefit of protecting users, while simultaneously removing friction within the authentication and account creation processes to varying degrees.

We’ve already touched on social login, so let’s discuss biometric authentication. Given the widespread adoption of biometric authentication within the finance sector, such as with the banking app on your phone, you’re probably familiar with it.

It replaces passwords (which can be leaked or stolen) with something that’s unfathomably hard to spoof. The unique shape and details of your customer’s face. Or the ridges, bifurcations, and arches that constitute their fingerprints.

These attributes are considered to be so unique, your bank is comfortable enough to use them in lieu of a password. From a UX perspective, they’re as close to friction-free as you can possibly get without compromising security. What’s easier than scanning your thumb, or raising your phone to your face?

Similarly, another type of passwordless authentication allows individuals to sign in to an account by simply clicking a unique, randomly generated link with a time-limited validity. These links are often referred to as “magic links.”

Also of interest to digital marketing leaders everywhere: The preference for passwordless is here.

The wider sample found 26% of US consumers reported using passwordless either all the time or frequently. For a global comparison, LATAM (42%), US (42%), and APAC (40%) consumers are more likely than their EMEA counterparts (29%) to sign up to an app/online service if they are able to use passwordless services.

This approach removes the need for end users to practice good password practices.

Perhaps the most well-known is multifactor authentication (MFA). This is another fundamental customer identity security feature. Put simply, MFA requires users to prove their identity during login by providing something only the user could possibly have, such as a one-time password sent to their mobile phone or a code generated by an external application.

MFA isn’t a silver bullet. There are ways to circumvent it. But it still adds an extra layer of protection. When done right, it can deter all but the most determined of threat actors.

It does, however, come with a UX cost. If your customer has to provide a unique token every time they authenticate, you’ve added friction—even if your motives are pure. Adaptive MFA can help. This means you only trigger a MFA when you notice something unusual, like if a customer logs in from a new location, or with a new device.

Like more modern approaches to customer identity, adaptive MFA strikes a balance between security and UX.

We probably sound like a broken record at this point. These features all have meaningful UX and security benefits. They remove friction and protect users at the same time. But their adoption remains limited.

> US organizations' progress in rolling out biometric logins and multifactor authentication (MFA) is ahead of organizations in APAC, EMEA, and LATAM, according to our survey.

Security and great UX can coexist: Here's how

If anything is clear from our analysis, it's that marketing leaders are aware of the critical business impact of UX and that many factors influence it. Identity is one.

Here's the good news: The nuances of securely handling authentication without frustrating consumers is a challenge that marketing leaders, are ready to take on. All that experience listening to customers is a great place to start.

Plus, there are software solutions that don't require weeks re-inventing the wheel just to implement MFA or social login. Modern customer identity solutions are what your customers are asking for and they do make everyone's life easier.

Tools like Okta Customer Identity Cloud are designed to deliver business value from day one and can implement the features that will delight your customers in a matter of minutes. Just as your customers will appreciate your improved UX, your engineering team will love how it simplifies identity-related development talks, reducing the time required to implement and maintain new functionality.

Curious to see how your login box is stacking up? Request a free in-depth assessment here.

About Okta
Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. For more information, go to okta.com.