Executive Summary

Most online retailers and digital businesses require customers to establish a digital identity for transactional or incentive purposes. This digital identity typically enables customers to have an account or record created that they can be securely authenticated against before accessing services. Most companies will use the personal information collected with these digital identities to take and fulfill orders, communicate with customers, provide individualized marketing and real-time personalization, and perform business analytics.

Companies must allow customers to manage these digital identities to adhere to a growing number of privacy regulations, such as the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). GDPR, for example, requires that companies must obtain consent from customers to use their personal information and give customers rights to view, modify, and revoke consent at any time.

Many organizations empower their customers to create and manage their digital profiles using a self-service process, which enables them to support customer preferences and a large number of customers at a low cost.

The Urgency

Preventing Account Abandonment

As customers set up and manage their digital identities, performing activities such as registration, account creation, login/password management, and preference management, they are likely to abandon the transaction if they encounter problems like insufficient usability, registration forms overloaded with too many questions, or simply slow load times.

Ease of use, performance, and reliability are vital to providing the experience customers expect. A study by Dynatrace and T-Mobile found that site visitors who experienced good performance were more likely to complete the transaction. Visitors are more sensitive to slower page speeds early in the customer journey. The registration, login, and authentication pages are among the earliest engagement points. These stages can more easily make or break the customer experience.

Use Case
Reducing Account Abandonment with Self-Service Identity Management
But user experience issues can occur at any stage of the customer journey. Forgotten passwords or issues with account updates or preference and consent management may impact customer satisfaction and result in account abandonment, decreases in brand loyalty, and lost business. Consumers who experience these challenges may opt for a costly phone call, email, or chat with customer service—or they may abandon the site altogether.

At the same time that they deliver good performance and reliability, companies must also keep customer data private and secure to meet regulatory requirements.

The Solution

Cloud-Based Identity Management Improves Customer Experience

Akamai Identity Cloud reduces account abandonment. As an Identity as a Service (IDaaS) solution used by some of the largest global brands, it enables hundreds of millions of users worldwide to establish and manage their digital identities with a good customer experience while complying with various regulatory requirements for data privacy and security.

With Identity Cloud, initial account setup is painless. It enables modern and flexible user experiences adherent to best practices, and it supports the option of social login. With social login, companies can pick from more than 35 social networks, such as Google, Facebook, Instagram, WeChat, and other identity providers. Updates a user makes on a social media site will also revise their account with the company.

If a user forgets their username and password, they can easily recover access via self-service without the need to contact customer service. Users can even employ social login account recovery tools. Step-up authentication ensures that the user asking for the password reset is really the account owner, preventing intruders from gaining access to someone else’s account.

Certain data privacy regulations require companies to enable their users to view, edit, and revoke the consent they’ve given to process their data, view privacy policies, and request their account be deleted. “It shall be as easy to withdraw as to give consent,” states article 7(3) of the GDPR.

In other words, providing an easy-to-use web form to collect consent in the first place and then making it purposely difficult to revoke consent afterward by requiring a complicated bureaucratic process is

91% of unsatisfied customers will not return for a repeat purchase or service

51% faster – the average page performance for customers who completed an order vs. those who started the transaction but did not complete it
not allowed. Identity Cloud enables customers to go into their account and effortlessly change their preferences, improving regulatory compliance and customer trust.

All of these user operations benefit from high performance and reliability. Identity Cloud boosts performance by intelligently caching data close to end users and employing elastic scaling to accommodate spikes in usage – it can easily handle millions of concurrent logins. Global availability (including Russia and China), a 99.95% uptime SLA, as well as sophisticated failover and BC/DR capabilities make Identity Cloud a solution specifically suited for large global brands.

Finally, powerful security enables state-of-the-art data protection. Strong encryption secures customer data in transit and at rest, and Identity Cloud’s edge protection capabilities provide protection against network-based threats, stopping attack traffic before it can reach the client’s application and cause outages, performance degradation, or cost increases.

User authentication, federated login, traditional login, two-factor authentication, or one-time-password (OTP) authentication can safeguard accounts. Access control capabilities verify access down to the level of user record fields, as well as by role and/or by attribute to reduce the risks of customer data exposure and improve data security. Identity Cloud even controls the flow of data to the applications it integrates with; for example, companies can restrict a marketing automation tool to accessing first name, last name, and email address, but no other fields, to prevent data sprawl and the accidental distribution of toxic data across the organization.

Visit akamai.com/identitycloud to learn more about how Akamai Identity Cloud improves the experience for customers as they manage their digital identities.

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 11/19.