Executive Summary

The State of Secure Identity Report 2023

Foreword: securing customer authentication

Rapid innovation and widespread access to information have revolutionized the demand for Identity solutions within the last decade. Identity is now the primary enterprise security entry point for consumer and workforce applications. Meanwhile, identity attacks have increased in volume and complexity. As an industry leader, Okta has a responsibility to champion a higher standard of identity security. The Okta Secure Identity Commitment is our long-term commitment to lead the industry in the fight against identity-based attacks. We will achieve this by providing market-leading secure products & services, hardening our corporate infrastructure, championing customer best practices and elevating our industry to be more protected from identity attacks.

In that context, this report aims to elevate industry understanding of key customer identity security trends, and share best practices.

Securing the login box is one of the most critical steps of identity security. Through **authentication**, an essential function of **Customer Identity and Access Management (CIAM)** services, the login box attempts to confirm a customer's **digital Identity** — the set of attributes that define a particular user (or non-human **entity**, like a specific device or system) in the context of an application.

But legitimate users aren't the only ones interested in what's behind the login gateway. There's money to be made for those who can break in, and economic forces have led to the emergence of an entire ecosystem of technologies, services, and other resources to enable such **intrusions**.

Across industries, attacks against entities large and small continue to accelerate. As cybercriminals direct more effort and expertise into getting past the login box — including by leveraging the same artificial intelligence (AI) capabilities that are transforming society and business — protecting it requires ever-more layers of ever-more sophisticated defenses.

Complicating matters is the reality that customer portals — whether business-to-consumer (B2C) or business-to-business (B2B) — generally have to be accessible on the public internet. Plus, the authentication experience has to be visible enough to create a sufficient level of trust for the customer, but seamless enough to not impose any unnecessary inconvenience.

For many years, customer authentication generally relied upon a knowledge factor — usually a password — presumed to be known only to the legitimate user and the application provider. But time and time again, this presumption has been proven false: knowledge can be stolen or learned (e.g., via **Open Source Intelligence**), passwords in particular are a problem, and both application providers and the CIAM services upon which they rely need to pull customers to more secure authentication factors. They also ideally need to get customers to enroll in **multi-factor authentication (MFA)**.

Up until a few years ago, an argument could be reasonably made that it was impossible (or at least impractical) to simultaneously satisfy the need for secure authentication with the imperative of a convenient user experience — that a trade-off was required — and that MFA was too unwieldy for widespread adoption, especially within B2C contexts.

But with the growing availability of **passkeys** — and **synced passkeys** in particular — we are now at the point where those arguments break down. In fact, we believe that the arrival of synced passkeys will be looked back on as a major milestone in securing **Customer Identity**. Plus, even setting aside their security benefits, passkeys have already proven to deliver a convenient and familiar user experience that, in many ways, surpasses the usability of other approaches.

And passkeys haven't arrived a moment too soon. Today, digital identities control access to an ever-growing number of applications and services, impacting — and to some degree governing — many aspects of modern living. Tomorrow, their impacts will be even larger, making authentication, **authorization**, and CIAM in general vital to preserving trust, security, and privacy. Consequently, CIAM also plays a central role in accessibility, and it's up to Identity practitioners to determine whether that role widens or helps to close the digital divide.

In this report, our third annual State of Secure Identity, we aim to increase awareness of threats to customer Identity and of the defensive measures that should be in place to withstand these threats. We've switched things up a bit this year, and structured the report as a three-part journey:

- Before the login box, because as much as the login box needs to be generally accessible, it really shouldn't be presented to everyone
- At the login box, where Identity battles rage every day
- After the login box, because securing access doesn't stop just because a user made it past the gatekeeper

Thank you for joining me — and all of us at Okta — on this journey.

Shiven Ramji

President, Customer Identity Cloud, Okta

Overview

CIAM is a unique segment of the wider Identity and Access Management (IAM) space, as customer-facing applications must deliver an experience that's user friendly, secure, and private while being fully exposed to an ever-changing threat landscape.

This report shows that signup fraud, credential stuffing, and MFA bypass are all everyday threats that must be managed by practically every customer login box.

The login box is a gold mine for bad actors

This report reveals that from January 1, 2023 through June 30, 2023...

13.9% of attempted account registrations met the Okta Customer Identity Cloud, powered by Auth0, criteria of a signup attack:

- Of the 10 industries with the most significant representation within the Customer Identity Cloud, four stood out as experiencing particularly high proportions of fraudulent registrations: Financial Services (28.8%), Media, (28.4%), Manufacturing (25.1%), and Software/SaaS/Tech (24.0%)
- On the “busiest” day for signup fraud, the Customer Identity Cloud identified nearly 10 million fraudulent registration attempts
- On April 15, more than 64% of account registration attempts were assessed to be fraudulent

24.3% of login attempts overall met the Customer Identity Cloud's criteria of credential stuffing:

- Of the 10 industries with the most significant representation within the Customer Identity Cloud, Retail/eCommerce (51.3%), Media (42.3%), Software/SaaS/Tech (32.1%), and Financial Services (30.3%) all experienced higher-than-average proportions of credential stuffing
- On the 'busiest' day for credential stuffing attempts, the Customer Identity Cloud identified more than 27 million such actions
- On January 1, more than 46% of login attempts were attributed to credential stuffing

12.7% of MFA attempts met the Customer Identity Cloud's criteria of being malicious (i.e., MFA bypass):

- Of the 10 industries with the most significant representation within the Customer Identity Cloud, Media (12.8%), Financial Services (10.9%), Manufacturing (7.8%), and Software/SaaS/Tech (6.4%) experienced the highest proportion of MFA bypass attempts
- On the "busiest" day for MFA bypass attempts, the Customer Identity Cloud identified more than 750,000 such incidents
- On June 11, MFA bypass attempts accounted for more than 30% of all MFA attempts

An organization's industry vertical isn't the only factor influencing the threats it faces. For example, small businesses and enterprises seem to be targeted at a higher rate — with fraudulent registrations, credential stuffing attempts, and MFA bypass attempts — than mid-market organizations. A reasonable interpretation is that cybercriminals consider enterprises as comparatively valuable targets and small businesses as comparatively easier targets.

And even the region in which an organization is headquartered has an effect: companies based in Asia-Pacific (APAC) experienced by far the highest rates of fraudulent registration, while those based in the Americas (AMER) faced significantly more credential stuffing.

		Fraudulent registration attempts[1]		Credential stuffing attempts[2]		MFA bypass attempts[3]	
		Rate	**Rank**	**Rate**	**Rank**	**Rate**	**Rank**
	Overall (technology wide)	13.9%	—	24.3%	—	12.7%	—
10 most-represented industries	Advertising/marketing	1.0%	10	16.7%	6	3.4%	9
	Financial services	28.8%	1	30.3%	4	10.9%	2
	Food/beverage/hospitality	9.0%	8	11.4%	8	5.5%	5
	Healthcare	6.3%	9	16.1%	7	4.6%	7
	Manufacturing	25.1%	3	17.7%	5	7.8%	3
	Media	28.4%	2	42.3%	2	12.8%	1
	Professional services	13.4%	5	7.2%	10	4.5%	8
	Retail/eCommerce	9.3%	7	51.3%	1	5.0%	6
	Software/SaaS/tech	24.0%	4	32.1%	3	6.4%	4
	Travel/transportation	9.7%	6	7.2%	9	2.9%	10
Organization size	Enterprise	19.9%	1	39.4%	1	9.5%	2
	Mid-market	12.6%	3	20.1%	3	9.0%	3
	Small business	19.4%	2	30.9%	2	20.3%	1
Organization HQ location	AMER	9.4%	2	28.0%	1	12.0%	1[4]
	APAC	27.9%	1	13.3%	3	11.0%	2
	EMEA	8.1%	3	20.2%	2	7.6%	3

Table 1: Summary of Identity attack rates as determined by the Customer Identity Cloud (January 1, 2023 through June 30, 2023)

[1] Proportion of total registration attempts
[2] Proportion of password authentication attempts
[3] Proportion of total MFA attempts
[4] Please see the Methodology section for an explanation of why all three regions are below the global average

Protect and delight customers with CIAM

While Workforce Identity management can accommodate comparatively higher friction and can often count on a user base that has undergone security awareness training, CIAM lacks these factors and must instead rely on more subtle security techniques to achieve and maintain a strong and resilient posture while preserving convenient user experiences.

Because customer expectations are always growing and the threat landscape is always evolving, these techniques must be continuously tuned to achieve the appropriate balance of user experience, security, and privacy — a balance that itself varies based upon each organization's risk profile and appetite.

Implement layered defenses

Basic controls — including rate limiting, suspicious IP blocking, and breached password detection — are all necessary defensive measures, but by themselves are insufficient.

Similarly, effective password policies (e.g., requiring strong passwords, having a secure reset process) and good session hygiene (e.g., keeping session tokens out of URLs, generating new and unpredictable tokens after login) are fundamental requirements, but only part of the solution.

As cybercriminals invest in bypassing security measures, CIAM services and application providers must also scale their investments in next-generation defenses.

For example, Bot Detection, with Okta AI has proven capable of filtering nearly 80% of bots targeting authentication systems. Importantly, these defensive capabilities were achieved without introducing unnecessary user friction: by carefully training and continually tuning the AI at the heart of the Bot Detection feature, we can ensure that human users are rarely presented with a CAPTCHA, preserving seamless experiences.

Plus, there's considerable evidence that this efficacy is a very strong deterrent: some of our largest customers saw their 90-day average of bot traffic drop by nearly 90% after enabling this Attack Protection feature — indicating that cybercriminals prefer going after easier targets.

Strengthen authentication

We can't overstate how much potential passkeys have to dramatically strengthen customer authentication compared to password-based logins. Passwords are at the root of many Identity threats, and passkeys represent a major step in relegating passwords to a much smaller role:

- Synced passkeys in particular deliver strong authentication in a familiar and convenient manner — making them beautifully suited to mainstream consumer demographics, which are especially sensitive to friction (in fact, as of October 10, 2023, Google offers passkeys as the default option across personal Google Accounts).
- **Device-bound passkeys** are a great option for B2B markets and other customer applications that require the even stronger authentication that comes from **FIDO** Certified authenticators and security keys

MFA in general also has a continuing role in strengthening customer authentication. In the past, customer-facing organizations were hesitant to introduce and encourage — let alone require — MFA out of concern that the consequences of additional friction would be too severe. However, those objections no longer apply (and really haven't for a few years):

- **Adaptive MFA** allows application providers to reserve MFA challenges only for risky logins, where riskiness is a function of many threat signals
- **Step-Up authentication** allows application providers to provide access to low-risk resources via a comparatively weaker authentication mechanism (e.g., a password), while reserving stronger authentication (e.g., MFA) for when a user wants to access a more sensitive resource

However — and as we've seen — threat actors are investing more resources in bypassing relatively weaker MFA factors, so it's essential that application providers migrate customers to authenticators based on possession or biometric factors.

Build or buy?

Building such a layered CIAM solution in house is a massive undertaking that's well beyond the capacity of all but the most well-resourced of enterprises. Nevertheless, such layers and technologies are required to deliver convenient and secure customer experiences that preserve privacy.

For most organizations, an agile, secure-by-design CIAM solution is the most effective and efficient approach, as it will allow them to tailor Customer Identity and Access Management — and continually tune as needed — without drawing in resources better applied toward advancing core competencies.

Third-party authentication makes a meaningful difference

A recent global survey of application development team members underscored the value of incorporating third-party authentication into SaaS applications.

Based upon 675 responses from professionals in 56 countries, the survey found that:

- **Authentication as a function takes the third-most time to build and maintain in house,** behind only Data Management and Storage, and DevOps Tooling and Automation
- **Third-party authentication reduces time to market more than any other SaaS component:** 88% of organizations that use a third-party SaaS platform for authentication report reducing time to market in the last year

Learn more in How development teams purchase SaaS

Enhancing customer security and experience with CIAM

Getting CIAM right — that is, implementing it in a scalable manner to satisfy the concurrent needs of user experience, security, and privacy — is a challenge for every organization:

- Because CIAM sits at the heart of customer-facing systems — serving as an input into market analysis and influencing acquisition, conversion, and retention efforts — it aligns with marketing and customer experience departments.
- At the same time, CIAM has a significant role to play in security and privacy, putting it squarely in the sights of CISOs, CIOs, and compliance officers.
- And — fundamentally — CIAM is a set of technology solutions, which causes it to fall under IT organizations, or even CTOs (when properly regarded as an enabler of digital transformation).

Leaders across these functions should work together to implement CIAM in a manner that balances quality of customer experience and system security, in the context of desired use cases, customer types, data types, industry-specific risks, and risk appetite.

Securing customer identities

Stopping today’s sophisticated Identity attacks and disrupting cybercrime business models — while preserving a good experience for legitimate users — is only possible by combining multiple security tools, operating at different layers, into a cohesive defensive posture.

Sourcing, integrating, configuring, and continuously monitoring, tuning, and orchestrating these tools on a solution-by-solution basis requires rare skills, consumes considerable operational attention, and pulls valuable resources that are better directed towards advancing a company’s core competencies.

For these reasons and others, a best-of-breed CIAM solution with an agile, secure-by-design, defense-in-depth architecture is a much more effective approach to achieving Identity security compared to building and maintaining an Identity stack in house.

10 Customer Identity best practices

Whether you are developing your own in-house solutions, or relying on an Identity-as-a-service provider, here are some fundamental recommendations:

- **Use generic failure messages:** Detailed failure messages can assist threat actors by providing information about users that exist in the system. Keep attackers in the dark by providing generic failure messages
- **Implement secure session management:** Use a server-side, secure session manager that generates a new session ID after login. Don't put session IDs in the URL, and do ensure they are securely stored and invalidated after logout
- **Don't ship with default credentials:** Default admin credentials are a major attack vector because many users leave them unchanged, leaving systems vulnerable to dictionary attacks
- **Don't store plain-text passwords:** If your password database is truly illegible, then it has no value to hackers. Encryption makes your organization a much less appealing target, but the implementation must be sound

Next, implement foundational defensive measures:

- **Limit failed login attempts:** Brute force attacks like credential stuffing often result in many failures for each successful login. Use this behavior to detect attacks and trigger countermeasures
- **Enforce strong passwords:** Many brute force attacks rely on weak or common passwords. Enforce password length, complexity, and rotation based on NIST recommendations or other evidence-based policies
- **Monitor for breached password use:** Many users reuse the same or similar passwords across multiple sites, so a breach in one service can threaten many others. Force users to change breached credentials

Finally, embrace stronger authentication mechanisms:

- **Champion passkeys:** Passkeys deliver robust authentication security, and synced passkeys offer the convenient user experience necessary to gain widespread adoption within consumer demographics
- **Offer strong MFA:** When introducing MFA, prioritize authenticator apps and WebAuthn-based methods; if you've already supported MFA for a long while, make an effort to migrate existing users to these stronger secondary factors, and away from legacy approaches
- **Adopt adaptive MFA and step-up authentication:** For organizations particularly concerned about any additional friction, these techniques help to achieve a finer balance between security and the user experience

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.

Auth0 is a foundational technology of Okta and its flagship product line – Okta Customer Identity Cloud. Developers can learn more and create an account for free at Auth0.com.

Disclaimer
These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, 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 any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

Any products, features or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.