



2023

Examining threats
against your customer
login box—and
everything behind it

The State of Secure Identity Report



okta

Table of contents

03	Foreword: Securing customer authentication
05	Executive summary
07	The login box is a gold mine for bad actors
09	Protect and delight customers with CIAM
13	Introduction to Customer Identity security
15	Consumers expect secure and convenient experiences
17	CIAM's role in security identities and applications
19	Adapting secure authentication to millions of peoples' desire for simplicity
21	AI has made it easier to deploy identity attacks at scale
23	Part 1: Before the login box
25	Host-layer defenses are the first line of defense
27	Platform and application layer defenses benefit from network effects
29	Part 2: At the login box
31	Sign-up incentives attract bad actors
39	Credential reuse aids attackers in account takeovers
59	Part 3: After the login box
61	Attackers value session tokens even more in a passwordless world
65	Enhancing customer security and experience with CIAM
69	Afterword: Authorization, the next frontier
71	Appendices



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



Executive summary

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.



Executive summary

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 technology 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 technology, 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 technology identified more than 27 million such events
- 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 technology, 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 technology 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 technology (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

Executive summary

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

Straightforward 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 additional friction would impede conversions. 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](#) ■

Introduction to Customer Identity security

Securing Customer Identity should be a top-tier priority for any application or service provider, for the simple reason that people other than legitimate users want access to whatever's behind your login box — and these malicious actors are willing to invest considerable effort to get what they want.

With this, our third annual State of Secure Identity Report, we aim to increase awareness of:

- Threats to Customer Identity
- The techniques available now that can be layered to build robust and reliable defenses

To achieve these goals, we'll explore today's most common and most dangerous attack patterns, and the broad trends that are shaping tomorrow's threat landscape.

Where possible, we'll provide data from Okta Customer Identity Cloud, powered by Auth0 — which provides CIAM functionality to thousands of organizations large and small — to illustrate the prevalence and impact of Identity threats.

But before we get into the specifics, it's worth taking a moment to review the unique context of Customer Identity, in particular:

- The need to deliver convenient experiences that are also secure
- The vital role of Customer Identity and Access Management (CIAM)
- The ongoing evolution of authentication mechanisms
- The double-edged sword of artificial intelligence (AI)



Introduction to Customer Identity security

Consumers expect secure and convenient experiences

For any organization serving customers through a digital channel, minimizing the friction inherent within each and every interaction is vitally important. In practical terms, this means minimizing clicks, designing intuitive user interfaces (UIs), reducing latency, and delivering a consistent and convenient user experience (UX) across the full range of channels (e.g., websites and apps).

To protect their services and legitimate customers, organizations must also implement security measures that can withstand a broad range of Identity-related attacks. An idealized Identity implementation provides infinite friction for attackers and something near zero — because a little bit of friction in the right place at the right time can help to build trust — for genuine users.

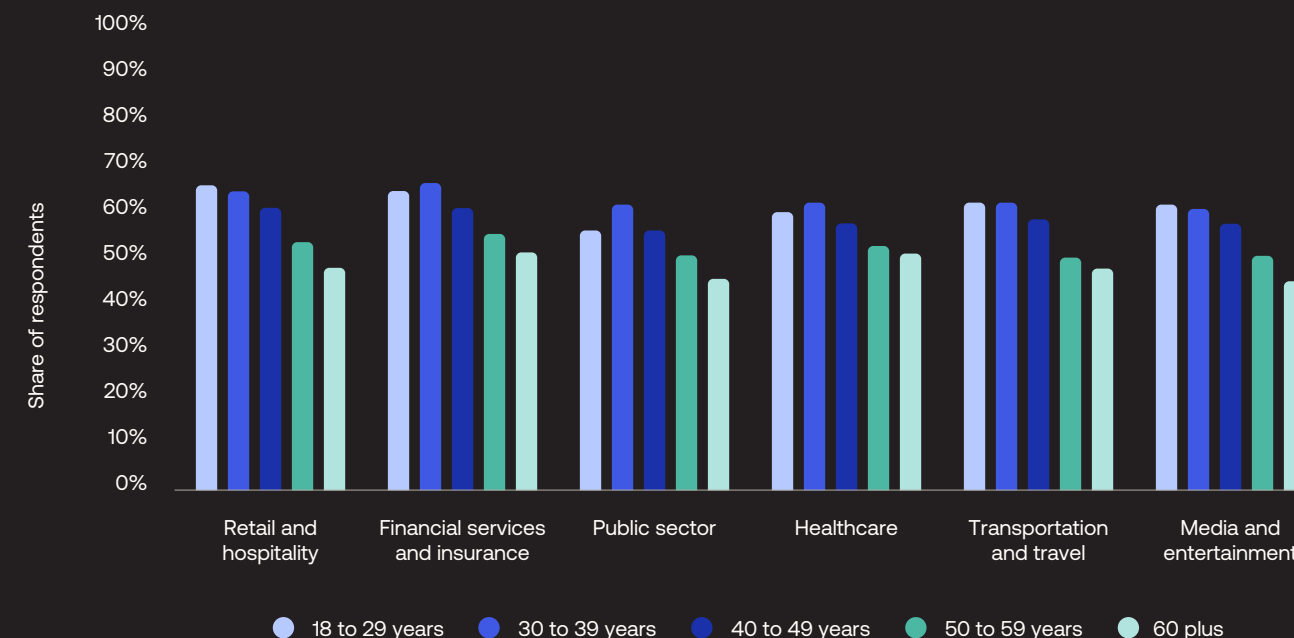
While such a solution is a worthy objective, the real world frequently involves tradeoffs. For example, deploying a mechanism to detect and impede large-scale, scripted bot attacks may increase an application’s overall resilience — but at the expense of some number of human users being presented with a security challenge.

Once deployed, the mechanism can be fine-tuned based upon operational insights to strike the appropriate balance between security and convenience. Practically, this balance will vary from application to application, organization to organization, and industry to industry, because each combination of customer base, threat landscape, and security preferences is unique. To complicate matters further, the balance may shift over time, as threat actors adjust their Tactics, Techniques, and Procedures (TTPs) and select new targets, and as customer desires shift.

But organizations that put in the effort and find a balance stand to reap significant rewards. For example, Okta’s [Customer Identity Trends Report 2023](#), based on a global survey of 21,512 consumers from 14 countries, revealed that nearly 60% of survey respondents would be more likely to spend money when services offered a simple, secure, and frictionless login process (Figure 1) — with the much-coveted younger demographics especially favoring such convenient experiences.

Figure 1: Consumers are more likely to spend money with a brand online if they know the login experience is simple, secure, and frictionless.

The graphs show the sum of “Very likely” and “Somewhat likely” responses.





Introduction to Customer Identity security

CIAM's role in securing identity and applications

A bot detection mechanism like the one outlined above is only a single element within an Identity security stack, and Identity security is only one aspect of Customer Identity and Access Management.

Modern CIAM solutions empower organizations to balance convenience, privacy, and security for every type of user who needs access to their applications and services. CIAM also allows companies to continually evolve the UX, to minimize the demand on the engineering team for Identity-related capabilities — thereby allowing them to focus on core features — and to efficiently and effectively meet regulatory, certification, and contractual requirements.

In Identity terms, the three essential features of an effective CIAM solution are authentication, authorization, and Identity management:

- **Proper authentication** ensures that the users logging into accounts are who they say they are.
- **Effective authorization** helps businesses to provide a user with the appropriate level of access to an application and/or resources.
- **Comprehensive Identity management** allows administrators to update user access permissions and implement security policies; this feature also enables customers to manage — to the extent permitted by the use case and required by regulations — their own identities, data, and preferences.

While the literal definition of CIAM has remained consistent, its true meaning — in terms of what use cases it enables, using what functional components, for what types of organizations — has evolved, especially in recent years. Today, CIAM is essential for:

- **Serving consumers:** In the business-to-consumer (B2C) world, an effective CIAM implementation enables highly personalized promotions and recommendations that drive additional revenue and create more value for your customers — all while ensuring a convenient user experience across your digital channels.
- **Empowering business customers:** Countless organizations rely on business-to-business (B2B) SaaS applications as essential enablers. However, different users within each organization need different levels of access to different resources, and creating a convenient and secure experience requires precisely managing Identity and access privileges. CIAM provides the answer by empowering B2B SaaS customers to self-manage Identity.
- **Enabling constituents, partners, and other known third parties:** In consumer and SaaS applications, customers manage their own identities, but there are many scenarios where Identity must be managed by the organization providing the service. To fulfill use cases where customer identities are known to, and provisioned by, the service provider, CIAM provides all the tools organizations need to manage customer account creation, maintenance, and end of life.

Within a Workforce Identity context, administrators can impose controls with comparatively less regard for the user experience. In the world of Customer Identity, the need to minimize (or at least carefully manage) friction creates challenges — particularly with respect to authentication.

Introduction to Customer Identity security

Adapting secure authentication to millions of peoples' desire for simplicity

While the Zero Trust paradigm represents a major change in the Workforce Identity world, CIAM has always operated in a world without trust. In almost every pure CIAM use case, neither the application provider nor the Identity provider has control over the endpoints from which the service is being accessed.

To establish enough trust to enable an interaction or transaction — i.e., to grant some level of access — Identity flows require each user to present one or more authentication factors:

- **Knowledge:** Something that the user knows, such as a password or the answer to a security question
- **Possession:** Something that the user has, such as a phone or access to an email account
- **Inherence:** Something that the user is, corresponding to a biometric attribute like a fingerprint, face, or voice profile; in most implementations, the device attests that the person attempting to authenticate is the same person who originally set up this type of authentication

But what started as a simple login box filled in by humans has changed dramatically over the years:

- **Passwords got more complex:** As attackers became adept at guessing weak passwords and taking advantage of widespread password reuse, requirements about complexity evolved, leading to ever-longer passwords with special characters, combinations of upper and lowercase letters, and numbers
- **Password management matured:** This forced users to grapple with more — and more complex — passwords, and drove adoption of password managers (whether implemented in a browser or in a separate application)
- **MFA's importance grew:** As **phishing** became a widespread threat and huge password dumps appeared online, MFA gained support as an effective defense against account takeovers (ATOs)

Unfortunately, the friction associated with traditional MFA techniques has resulted in low consumer adoption; plus, many older MFA techniques are now under threat, with attackers finding scalable and economic ways to bypass this important barrier.

As authentication techniques and attacker TTPs evolved, CIAM solutions introduced new layers of Identity security to defend against a wide array of automated cyberattacks that both cost organizations money and that threaten the privacy of customers.

Inching ever-closer to the idealized solution, modern security measures include approaches like adaptive MFA and step-up authentication — both of which aim to only create friction when a sufficient level of risk exists. Key to deciding exactly when a security challenge is needed — that is, to maintain the optimal balance between security and convenience — are intelligent systems that ingest risk signals and other context (e.g., the level of access being requested) to assess risk, choose an appropriate authentication challenge, and so on.

In fact, artificial intelligence (AI) has long been embedded within Identity systems, and AI's importance is undoubtedly going to increase (even looking beyond security, AI can be leveraged to craft better customer experiences).

However, while AI is many things, it's also just another tool that can be wielded for good or ill.



Introduction to Customer Identity security

AI has made it easier to deploy identity attacks at scale

On a basic level, artificial intelligence can be understood as a decision made by a computer where its “smartness” is indistinguishable from a human-made decision — no matter how the decision is made.

The original premise can be traced back to 1943, long before the invention of the digital stored memory computer, when logician Walter Pitts and neuroscientist Warren McCulloch [tried to create a mathematical representation of the neurons in a human brain](#).

Since the 1960s, AI has evolved into a very large collection of algorithms, which can perform various tasks. One of those tasks is the detection and recognition of patterns, and is usually called machine learning (ML). The ML field has advanced quite dramatically in the last 15 years due to progress in the construction and manipulation of neural networks — and with ever-more powerful computers, neural networks can be made “deeper” (or larger), resulting in the emergence of practical and economic deep learning.

But the AI development that has taken the wider world by storm is the incredible — and many would say shocking — arrival and rapid evolution of generative AI, driven mainly by remarkable advances in Large Language Models (LLMs).

Suddenly, writing prose and creating complex (and lifelike, if that’s the intention) images are no longer the sole domain of humans. And what’s more, because

LLMs are so adept at writing — including programming — and so many things are now controlled by software, [LLMs are behind unexpected breakthroughs and advances](#) in a wide range of domains.

In the context of Identity security, advances in AI make the threat landscape more dangerous in a few ways. For example, AI can:

- **Make existing low-quality, high-intensity Identity attacks more dangerous:** Credential stuffing, fraudulent registrations, SMS pumping schemes, and other attacks may become harder to detect, and more effective/destructive
- **Enable entirely new types of Identity attack:** Some new attacks will be anticipated by defenders or discovered in advance by researchers, but others will only become apparent once they’re spotted in the wild (i.e., the “unknown unknowns” problem)
- **Overcome some existing security measures:** AI-based tools have already demonstrated the ability to solve CAPTCHAs and to use trick voice biometric systems via deepfakes

Plus, the coding and scripting abilities of generative AI makes it easier for threat actors of any skill level (i.e., with or without coding abilities) to launch attacks, in general, potentially drawing more participants into the cybercrime ecosystem and improving their operational efficiencies.

Enabling scalable and cost-effective personalized attacks

But perhaps the most dangerous new Identity threat is that AI enables **spear phishing** at a massive scale. Consider this plausible attack pipeline:

1. A threat actor selects an organization to target
2. The threat actor uses **open-source intelligence (OSINT)** techniques to compile a list of employees
3. The threat actor feeds this list into a social search API (there are many options available), which then returns a list of social media accounts associated with each employee
4. The threat actor programmatically filters the list to identify employees with open and active social media accounts, then starts examining each to identify who the user follows, what posts they like, what they post, when they’re active, etc.; the threat actor can even perform subject-based sentiment analysis to build highly personalized psychological profiles, and can update these profiles over time
5. The threat actor follows each employee on the available social applications, and begins interacting in completely benign ways (e.g., liking and resharing posts, adding comments, etc.) to establish a rapport
6. The threat actor monitors current events, news, and trends for an opportunity to engage with each employee on a personal level
7. The threat actor crafts an email (or direct message, on any medium) and reaches out to each target employee
8. If a target engages, then the conversation can continue until enough trust has been established that the threat actor can make a request with a high probability of success

Even until the recent past, executing such an attack chain was a tedious, manual, and expensive endeavor; today, it can be nearly completely automated and executed at scale — personally targeting thousands of employees across many organizations — [for very little cost](#).

Strengthening defenses

Fortunately, while AI will undoubtedly aid attackers, it also serves as a ‘power-up’ for defenders. For example, AI can be employed to:

- **Further secure applications by design:** Just as threat actors can use AI to probe for vulnerabilities and security gaps, so too can application providers — with a first-mover advantage of hardening software and systems before they’re released.
- **Improve automated threat detection:** Contextual and behavioral analysis is already capable of informing intelligent risk assessments and detecting advanced Identity threats, and advances in AI will only improve the ability to perform these functions and to introduce new ones.
- **Mitigate risk:** Whether automating defensive measures (e.g., containment actions, blocking malicious activities) or combining an alert with a recommended playbook, AI will be invaluable in proactively mitigating risk and responding to attacks.

With the stage set, let’s start our journey to the login box — and beyond. ■

Part 1: Before the login box

The goal of these initial defenses is to prevent any illegitimate entity — human or machine/system — from being able to access the login interface.

The earlier a malicious entity can be filtered out, the better, as doing so reduces computation costs and limits the reconnaissance that the attacker can perform (e.g., by receiving and analyzing error messages).

To that end, a number of defensive measures exist across different layers of the Identity infrastructure:

- **Hosting defenses**, which are applied by the hosting provider (e.g., Microsoft Azure, Amazon Web Services) or at the hosting layer (e.g., Cloudflare)
- **Platform defenses**, which apply across a CIAM platform as a whole (e.g., Okta Customer Identity Cloud)
- **Application defenses**, which apply across a single CIAM application (e.g., home-built, point solution)



Part 1: Before the login box

Host-layer defenses are the first line of defense

Hosting providers offer a number of security features intended to prevent abuse of the services they host, including:

- **Distributed Denial of Service (DDoS) mitigation:** Protections help your CIAM application to remain available to legitimate users, even in the face of large-scale attacks (particularly at the TCP/UDP layer)
- **Bot management:** An initial layer of bot filtering is typically based upon a combination of behavioral analysis, threat intelligence, and feedback loops
- **Rate limiting:** Controls help protect against DoS attacks, brute-force strategies, and API abuse by imposing restrictions on the rate at which a particular entity can access the CIAM platform/application



Part 1: Before the login box

Platform- and application-layer defenses benefit from network effects

These defenses exist on a spectrum from tactical to strategic, and are most effective when used in combination and when customized to specific needs.

They also benefit enormously from network effects. A CIAM platform providing Customer Identity services to hundreds or thousands of organizations can directly gather many orders of magnitude more threat intelligence than an isolated CIAM application, to the benefit of every organization on the platform. For example, IPs observed attacking one tenant can be blocked across all tenants.

Rate limiting

Rate limiting (throttling) is a useful tool for countering high-volume, brute-force attacks by imposing restrictions on the rate at which a particular entity can interact with the CIAM platform as a whole, or with the CIAM application of individual organizations.

In either scenario, when an entity exceeds a prescribed threshold (e.g., some maximum number of attempts in an hour), they can be:

- Required to complete a challenge (e.g., CAPTCHA)
- Restricted from accessing the login interface until a ‘cooling off’ or ‘penalty’ period has passed

Plus, rate limiting is also effective at limiting the impact of DDoS attacks that target the Identity service.

For sites and services whose functionality is gated behind a login, overwhelming the authentication service has the same outcome as any other type of DoS attack — denying the ability for legitimate customers to use the service.

Suspicious IP blocking

Blocking suspicious IPs from accessing Internet-facing services has been employed for decades and still has utility today — provided its limitations are recognized.

The approach is simple:

- Some factor is used to determine if an IP address can be trusted
- Addresses that fall below a prescribed trust threshold are denied access to the application

The same general technique can be applied to phone numbers, email addresses (for example, some applications only allow users from paid email services to register), and other variables.

To facilitate such filtering, many organizations subscribe to cybersecurity threat intelligence (CTI), some maintain a proprietary list of reputations based upon their own direct observations, and others combine these approaches.

Bot detection

Bot traffic plagues Identity flows at all points of the user journey. More than being a nuisance (to put it lightly), it also has a hidden cost; consider that the Customer Identity Cloud sees billions of bot-initiated login requests every month, which equates to potentially millions of dollars in compute costs borne by application providers just to accommodate that bogus traffic.

By analyzing a variety of data sources and observations, it’s possible to determine with high confidence when a connection attempt is coming from a bot.

In such a scenario, the request can be blocked or ignored outright, or the entity can be presented with a challenge like a CAPTCHA.

Using machines to fight machines

As a vital part of the [Attack Protection](#) add-on in the Customer Identity Cloud, the [Bot Detection](#) feature mitigates scripted attacks (e.g., credential stuffing, password guessing, password spraying) against native applications, **passwordless** flows, and custom login pages.

By analyzing more than 60 data sources — like past events associated with an IP address, recent login history, IP reputation data, and an assortment of other factors — Bot Detection predicts when an Identity request is likely to be coming from a bot. Above a certain prediction/confidence threshold, the authentication flow presents a countermeasure, such as a CAPTCHA.

Bot detection is a terrific example of how AI can improve upon prior techniques:

- The first version, introduced in February 2021, was rules-based and detected 18% of bots
- Version two, which debuted in August 2021, employed machine learning for behavioral analysis; this AI-powered approach more than doubled the effectiveness, detecting 45% of bots
- The most recent version, launched in June 2022, [detected 79% of bots](#) — the highest performance yet, despite threat actors continually refining their own techniques

Importantly, these improved 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.

Plus, a detailed internal study examining the before-and-after effects of Bot Detection has revealed a strong deterrent effect:

- On average, customers in the study who enabled Bot Detection saw a reduction in malicious traffic of more than 40%
- Some larger customers in the study saw bot traffic drop by nearly 90%

These findings suggest that threat actors prefer to avoid targeting organizations with state-of-the-art defenses in place. ■

Part 2: At the login box

Entities that make it to the login box have already overcome a series of hurdles designed to filter out malicious actors. Once here, there are two actions a legitimate user may pursue:

- Sign up for an account
- Sign in to an existing account

As we'll see, threat actors routinely target both services.



Part 2: At the login box

Sign-up incentives attract bad actors

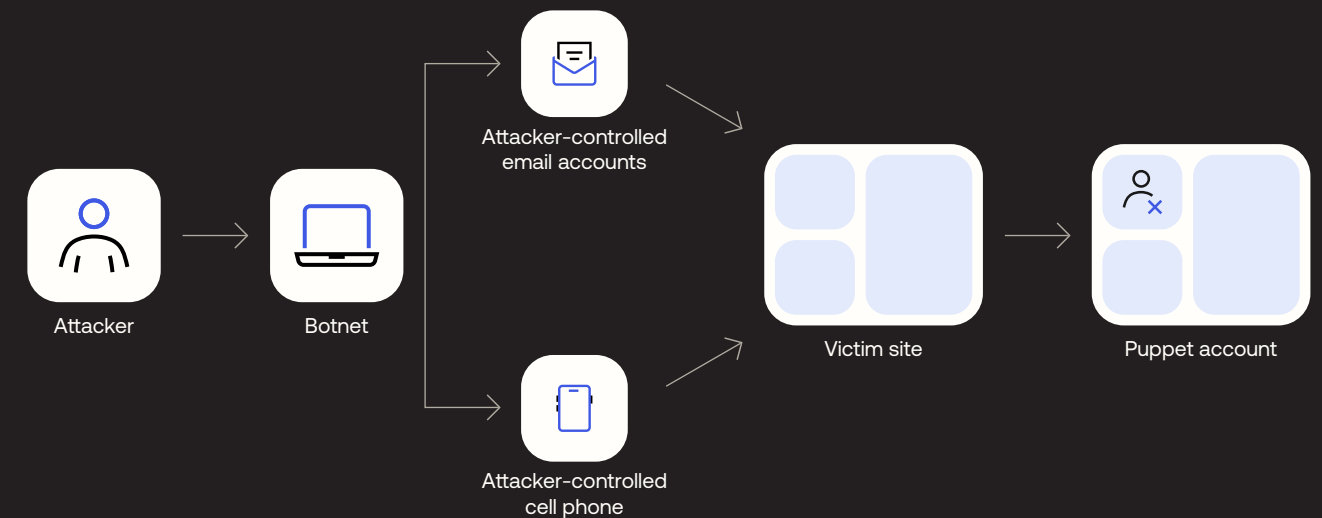


The easiest way for a malicious user to access the privileges, services, and information behind the login box is to create puppet accounts under their control from day one.

There are a number of potential motivations for doing so, including:

- **Gaining inequitable access to something valuable**, like limited edition sneaker drops, concert tickets, new video game consoles in short supply, etc.
- **Receiving awards or incentives that are associated with account creation**, including gift cards, cryptocurrency tokens, etc.
- **Spamming, disinformation, or hacktivism campaigns** that leverage accounts to participate in comment threads or to amplify messages
- **Committing synthetic identity fraud**, which often leverages financial services and utilities accounts
- **Reselling accounts** to interested parties
- **Harming the application provider’s ability to deliver services** by exhausting the namespace of potential users, and thereby preventing legitimate users from registering
- **Optimizing ATO attacks** by using the puppet accounts to carefully manipulate login success and failure rates to bypass automated security measures

Figure 2: Anatomy of a fraudulent registration attack



Fraudulent registration predominantly targets organizations that operate in a B2C context, particularly those in which a user can create an account for free and without any precondition (e.g., a proof of purchase).

Especially when performed at scale, fake signups can create significant problems and lead to unnecessary expenses.

First, fake users may negatively impact the experience of legitimate users (e.g., by scooping up in-demand products), leading to customer dissatisfaction and reputational damage for the business; plus, they consume resources and may abuse their access to directly attack or harm the organization.

Second, because one of the major objectives for B2C organizations is to turn prospects into first-time customers, entire conversion flows are often optimized based upon analytics data that shows how users interact with the service. Fraudulent registrations

pollute this data, significantly complicating business analytics activities and potentially leading to expensive clean-up projects.

Unfortunately, because B2C organizations (in particular) are so dependent upon maximizing conversion rates, there’s a major incentive to minimize friction during the registration process — but reducing friction for legitimate users also lowers the barriers for abusers.

The attacker may seek to create only a relatively small collection of puppet accounts or could employ a botnet to automate the creation of vast numbers — e.g., thousands or even millions. In the latter scenario, the operation may be aided by lists of common usernames.

A sudden surge in failed signups (or in the failed signup rate) is a strong indicator that your application is under attack. In this situation, you may wish to take a closer look into the registration traffic to see if thresholds or rules should be modified.

Aggregate observations

Figure 3 shows an aggregate (i.e., technology-wide), 30-month view of fraudulent registration attempts. Even at a glance, two major characteristics stand out:

1. Fraudulent registrations are an ever-present plague upon customer signup services
2. The volume of fraudulent registrations (and, accordingly, their ‘contribution’ to total signup attempts) varies wildly from one day to another

Slightly less obvious are two important trends.

First, the peak daily proportion of fraudulent registrations has declined over that same period:

- In 2021, it was all-too-common (93 occasions) for fraudulent registration attempts to account for the majority of total registration attempts on a given day, and there were 19 instances in which fraudulent registration attempts accounted for more than 70% of registration attempts
- In 2022, fraudulent registration attempts represented more than 60% of signup attempts on only five occasions
- In the first half of 2023, only one day (April 15) saw more than 50% of registration attempts deemed fraudulent

Second, the proportion of total registration attempts attributed to fraudulent registrations has declined significantly in this 30-month window:

- In 2021, 31.8% of registration attempts were determined to be fraudulent
- In 2022, this proportion had declined to 18.6%
- In the first half of 2023, the proportion had dropped to 13.9%

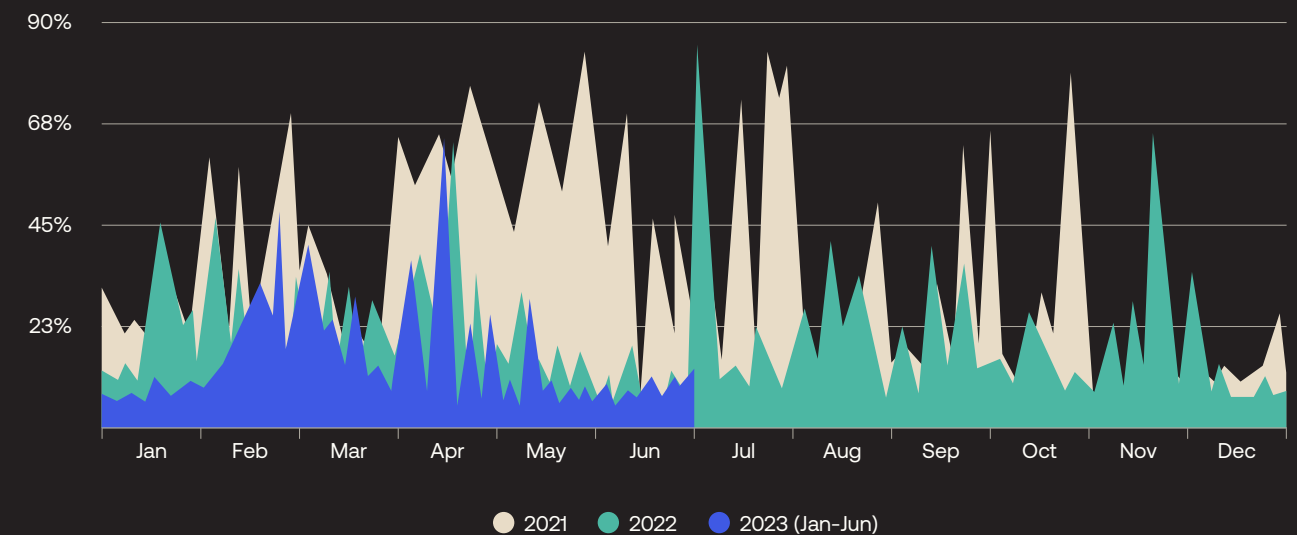
We believe that the primary reason for these positive trends is continued improvement to the technology’s layered defenses, rather than a major reduction in attempts by malicious actors to set up fraudulent accounts (we will [return to this hypothesis](#) shortly).

It’s also important to recognize that only the most egregious offenders reach the required thresholds to be considered fraudulent; moreover, once an entity has been identified as engaging in a signup attack, many tenants implement controls that prevent malicious signup attempts — when this is the case, these attempts don’t even get the opportunity to contribute to the count/log of fraudulent signup events.

Additionally — and please forgive the repetition, but it really is an important point — malicious actors have already run a gauntlet of host, platform, and application defenses before they can even see the login screen.

For these reasons, the percentages mentioned above and shown in the figures below should be regarded as the absolute minimum; realistically, a signup service lacking layers upon layers of effective defenses is at severe risk of being inundated — if not overwhelmed completely — by scripted account registrations.

Figure 3: Fraudulent registrations are an ever-present threat, but represent a declining proportion of total registration attempts on the Customer Identity Cloud due to enhancements within our product suite



Segment analysis

Deeper inspection of the underlying data reveals that fraudulent registration attempts are unevenly distributed.

Of the ten industries with the most significant representation within the Customer Identity Cloud, Financial Services (28.8%), Media (28.4%), Manufacturing (25.1%), and Software/SaaS/Tech (24.0%) all experienced higher-than-average proportions of fraudulent signup attempts (Figure 4).

Why are accounts within these industries so highly valued by attackers? There’s no convenient way to know for sure, and the answers may well be many and varied, but here are some potential explanations:

- Financial Services providers and institutions often include welcome bonuses and other perks (e.g., travel points, lower interest rates) with new accounts, and anything with monetary value is attractive to cybercriminals. Accounts may also be used to facilitate money laundering and as stepping stones for synthetic Identity fraud.

- Media outlets frequently have comment forums, so controlling accounts provides an opportunity to spread disinformation, hate messages, propaganda, spam links, and other malicious content to a wide audience.
- Manufacturing organizations are highly targeted by cybercriminals, as any production disruption applies pressure to meet ransom demands — so it’s possible that at least some fraudulent accounts are created as part of longer attack chains. Plus, manufacturers who sell directly to consumers may offer special access to production runs or items in limited supply, creating an incentive for prospective resellers to create a horde of accounts.
- Many Software/SaaS/Tech services use a freemium model that places limits on one or more factors (e.g., hours of use, volume of storage, available computational resources, etc.); perhaps fraudulent accounts are attempts to evade these restrictions.

Note: Additional context for industry-based analysis is available in [Appendix C](#).

Curiously, enterprises and small businesses appear to experience a meaningfully higher proportion of fraudulent signup attempts than do their mid-sized counterparts (Figure 5).

We can speculate that cybercriminals may reasonably expect enterprises to be well-defended (i.e., relatively smaller chance of success), but the payoff from a successful attack is high enough that the return on investment (ROI) justifies the effort.

Cybercriminals follow the same economic incentives as legitimate organizations, and are looking to maximize their profit, so the observations suggest that the expected value of engaging in signup fraud against enterprises and small businesses exceeds that of targeting mid-market businesses.

Small businesses may offer the opposite situation: a lower payoff per attack, but with a sufficiently high expected rate of success to be worth attacking.

Note: Additional context for analysis based on organization size is available in [Appendix D](#).

Likewise, more differences appear when we aggregate by the region in which an organization is headquartered (Figure 6). Organizations based in the Americas (9.4%) and EMEA (8.1%) experience comparatively much lower proportions of fraudulent registration attempts, relative to organizations headquartered in APAC (27.9%).

Such a stark disparity between APAC and the other regions may be a symptom of a less mature approach to Identity security, which manifests as enabling fewer security products and features in the account registration pipeline.

Note: Additional context for region-based analysis is available in [Appendix E](#).

Figure 4: Financial Services and Media companies experience a higher-than-average proportion of fraudulent registration attempts

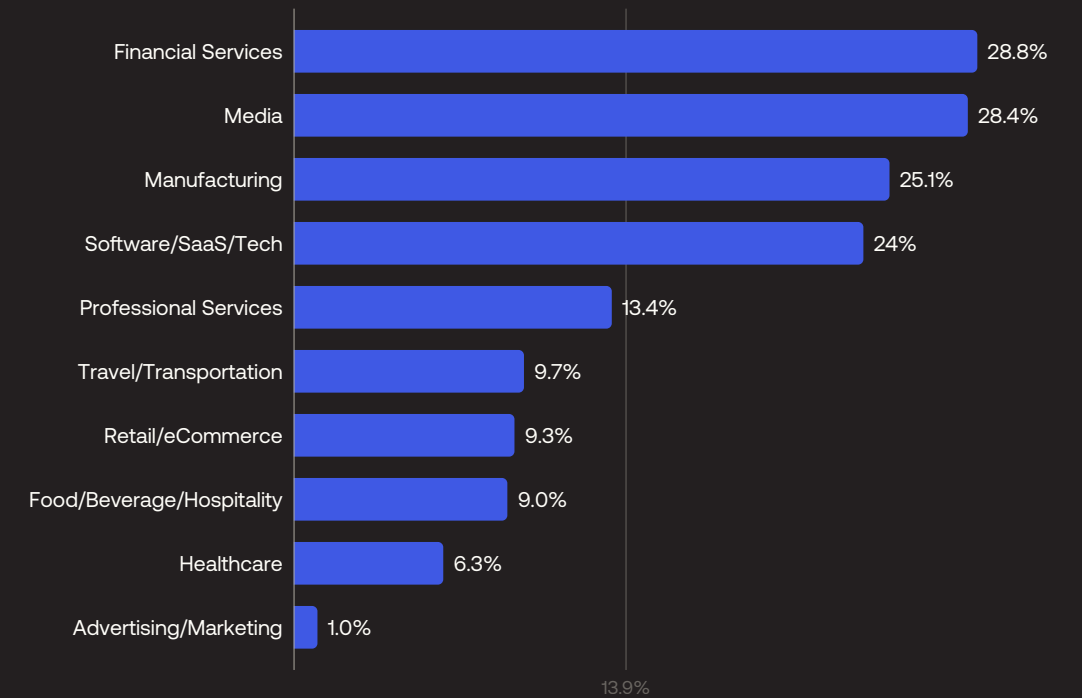


Figure 5: Fraudulent signups seem to be especially prevalent for enterprises and small businesses

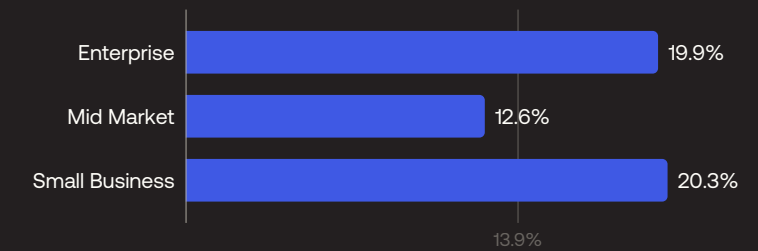
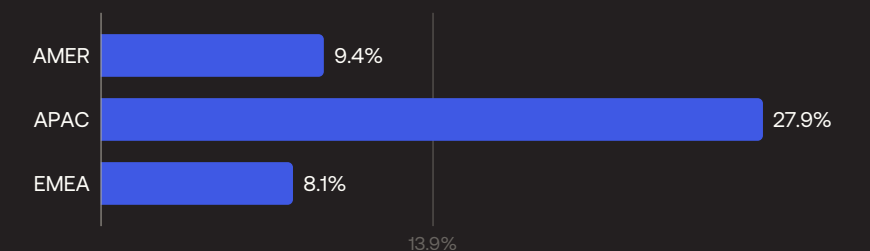


Figure 6: Organizations based in APAC experience a much higher proportion of fraudulent signup attempts than those based in the Americas or EMEA



Defensive measures

Beyond the defensive layers that exist prior to accessing the login box, there are several other approaches that can be applied to reduce fraudulent registrations, including:

- **Pre-signup rules and actions** (e.g., enforce a challenge, require more information) to further reduce the chances that a new user is illegitimate
- **Social login** to ‘outsource’ prevention of fraudulent signups
- **Identity proofing** when risk is perceived to be particularly high
- **Validating contact information** (e.g., email address, phone number), for example through a one-time passcode or **magic link**

Crucially, intelligence gained from signups that fail — for a variety of reasons — should be fed back into the overall threat intelligence assessment. For example, an IP that tries and fails to register some predetermined number of accounts (e.g., 10) within some window of time (e.g., one hour) should be deemed risky — with the “risky” designation leading connection attempts from that IP to be filtered at the platform or application level (i.e., before the login box).

However, aside from social login, each of the approaches listed above introduces additional friction into the signup process — so care must be taken to strike the appropriate balance.

Additionally, organizations need to be mindful that threat actors have begun to abuse SMS and call-based validation methods (as explained below).

Threat spotlight: SMS pumping and toll fraud

The ubiquitous availability of SMS makes it an attractive channel for Identity flows. For example, many sites have signup flows that incorporate or allow only SMS-based registration (e.g., Toast, Uber), and SMS is a popular mechanism for delivering registration and MFA challenges (e.g., **OTPs** and magic links).

Unfortunately, threat actors are abusing form fields to trick application providers into sending SMS messages or phone calls to premium numbers — allowing them to pocket a share of the proceeds.

In both cases, the organization whose application is being abused incurs the costs, which can be significant — in February 2023, [Elon Musk claimed](#) that Twitter was losing \$60 million USD per year due to “fake 2FA SMS messages.”

As with the other attacks explored within this report, threat actors have discovered tactics that reduce the risk of detection. For instance, they may:

- Rotate through phone numbers, to avoid exceeding per-number thresholds
- Go low and slow, stretching the attack out for many days, weeks, or months (really, as long as they can before getting caught)

Many organizations rely on SMS during user signup and authentication, so simply switching off this channel isn’t a practical option; instead, the Identity infrastructure must include a highly intelligent way to prevent or mitigate telephony-based fraud.

Social login

Social login provides **single sign-on (SSO)** for end users. Using existing login information from a social network provider like Facebook, Twitter, or Google, the user can easily register for (and subsequently sign into) a third-party service instead of creating a new account.

In addition to giving end users a convenient experience, social login can help to combat signup fraud — *if the login provider has implemented strong signup security measures.*

The challenge is that services will vary in this regard, forcing application providers to decide which third parties are trustworthy.

Notably, social login also provides other potential benefits to application providers, including:

- **Increased registrations:** Many users prefer reusing an existing account over creating another new one
- **Verified email:** The social network provider is in charge of verifying the user’s email. If the provider shares this information, then you will get a real email address rather than the fake addresses often used to register in web applications. Social providers will also handle the password recovery process
- **Greater personalization and customization possibilities:** Social network providers can give you additional information users have consented to share, such as location, interests, birthday, and more, which you can use to enhance your services
- **One-click return experience:** After users register in your application using Social Login, their return experience will be very simple, as they will probably be logged into the social network, and just one click will be enough to login to your application

Identity proofing

One of the most common misconceptions in CIAM is that authentication and Identity proofing are equivalent; however, while authentication (e.g., signing in with a username and password) shows that a user has the credentials that correspond to a particular account, it doesn’t prove that the user is who they say they are. That’s where Identity proofing comes in.

Identity proofing uses additional verifications to create a high degree of confidence that your prospective registrants are who they claim to be.

Within the CIAM context, it’s important that Identity proofing solutions scale, because CIAM typically demands real-time workflows to accommodate the spikes associated with seasonal variation and successful promotional programs. Fortunately, in recent years a number of automated Identity proofing techniques have been developed to meet the real-world demands of customer registration:

- **Knowledge-based authentication (KBA)**, which leverages something a user — and, ideally, only that user — knows
- **Document scanning and cross-validation**, which uses a trusted photo ID — for example, a passport or driver’s license — to verify that a user’s claimed Identity matches their actual Identity
- **Phone carrier verification**, which takes advantage of the fact that the user’s Identity was already proven when they signed up for a phone service

Part 2: At the login box

Credential reuse aids attackers in account takeovers

While fraudulent registrations are (at a minimum) an expensive nuisance, account takeover poses a greater threat to security and privacy.

In a B2C context, attackers may gain access to resources (e.g., loyalty points), privileges (e.g., ability to make purchases, especially of products in limited supply), and valuable demographic and personally identifiable information (PII).

In a B2B context, an attacker who successfully compromises a user account may use it to access highly sensitive data, resulting in a breach with severe regulatory and contractual penalties for the targeted organization.

Although some ATO attempts target individuals (we'll examine some approaches in Part 3), most are brute-force attacks (e.g., T1110) employing one or more of the following techniques:

- **Credential stuffing** (e.g., T1110.004): a threat actor tries known credentials (i.e., from a breach/dump) across other sites and services
- **Password spraying** (e.g., T1110.003): a threat actor tries a comparatively small list of the most common passwords across many different accounts
- **Password guessing** (e.g., T1110.001): a somewhat cruder approach in which a threat actor tries many passwords across any number of accounts

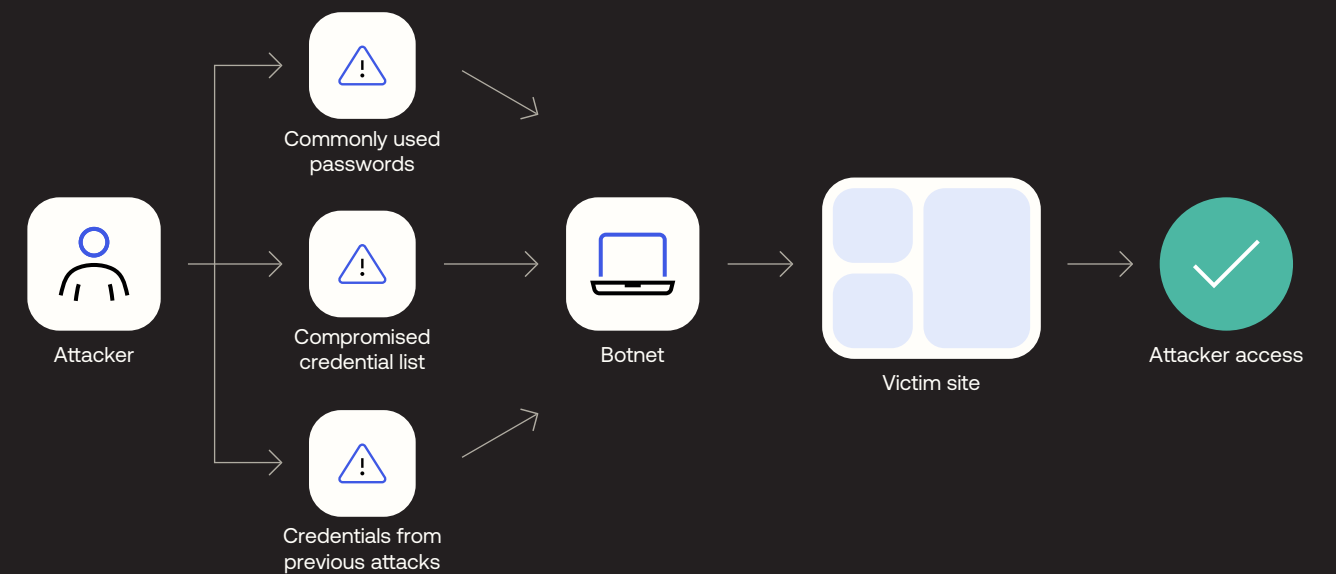
Note that any of these attacks, executed at sufficient scale, may have the effect — whether intended or not — of slowing authentication for legitimate users, or rendering the authentication service completely unavailable.

All three approaches rely upon users engaging in poor password habits (e.g., simple passwords, reusing passwords), a prevalent problem that dramatically reduces the cost and effort associated with launching these attacks. For example, a small number of optimizations — including leveraging lists of breached passwords and dictionaries of words that are frequently used within them — can dramatically improve the likelihood of trying the correct password (or, more accurately, of trying a password that hashes to the same value as the correct password).

Of the three attacks outlined above, credential stuffing is the most effective (from the standpoint of the threat actor) and dangerous (from the perspective of the application provider and its customers), because it's more precise. By trying known username and password pairs, a threat actor is somewhat less likely to trigger automated detection mechanisms.

Unfortunately, the barrier to launching such attacks is very low, and threat actors employ a number of tactics to try to evade defenses. For example, an attacker may intersperse known valid credentials — perhaps from fraudulent accounts already under their control — into the login stream to carefully manage the failure rate:

Figure 7: Anatomy of a credential stuffing attack



For the more sophisticated threat actor, credential stuffing attacks are desirable because there is almost zero marginal cost. Consider a kill chain extended from Figure 7, in which the threat actor uses a cybercrime service to launch a phishing campaign to acquire credentials. The harvested credentials are known to be active at the moment of harvesting, which enables the threat actor to launch a credential stuffing attack with a high expected rate of success. In this scenario, targeting different organizations and services is as simple as changing a few parameters within a script.

In addition to account takeovers, credential stuffing is often employed for the intermediate step of account discovery/validation. For example, a threat actor can take a large credential dump, run it through a particular service, and then sell the validated list for a premium price.



Aggregate observations

Figure 8 shows a 30-month view of credential stuffing attempts on the Customer Identity Cloud. As was the case with fraudulent registration attempts, cursory visual analysis suggests that the proportion of login attempts attributable to credential stuffing has declined significantly in that period — and that is indeed the case:

- In 2021, 42.8% of login attempts were attributed to credential stuffing (as with fraudulent signup attempts, the criteria that must be met to receive this label are very strict and — once flagged as such — additional attempts aren't even logged)
- In 2022, the proportion was 33.4%
- In the first half of 2023, the proportion dropped to 24.3%

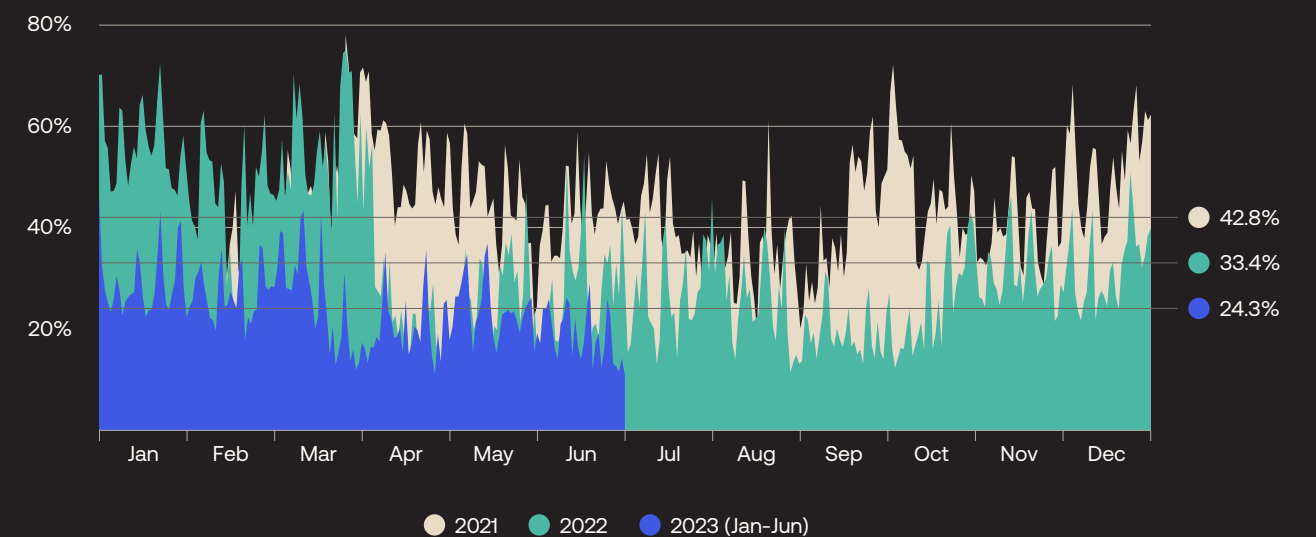
Closer inspection reveals that a major change occurred in April 2022:

- From January 1, 2021 through March 31, 2022, credential stuffing accounted for 47.3% of login attempts
- From May 1, 2022 through June 30, 2023, only 24.6% of login attempts met the criteria of credential stuffing

So what happened in April 2022? In short, during the first two weeks of the month, the order in which the Consumer Identity Cloud's defensive layers filtered out attack traffic was changed — with Bot Detection getting 'promoted' to apply earlier in the pipeline.

We believe this single change is responsible not only for the dramatic and sustained reduction in credential stuffing and other brute force attacks against the login box, but also for much of the improvements noted in the analysis of Figure 3 (relating to fraudulent registration attempts) — which underscores not only the importance of having multiple defensive layers, but of optimizing how those layers are organized.

Figure 8: The proportion of login attempts attributable to credential stuffing has declined significantly in 2023. Improvements to the Bot Detection feature in Customer Identity Cloud could be behind the decrease.



Segment analysis

Segmenting the technology-wide observations by industry (Figure 9) underscores how especially problematic credential stuffing is for certain industries.

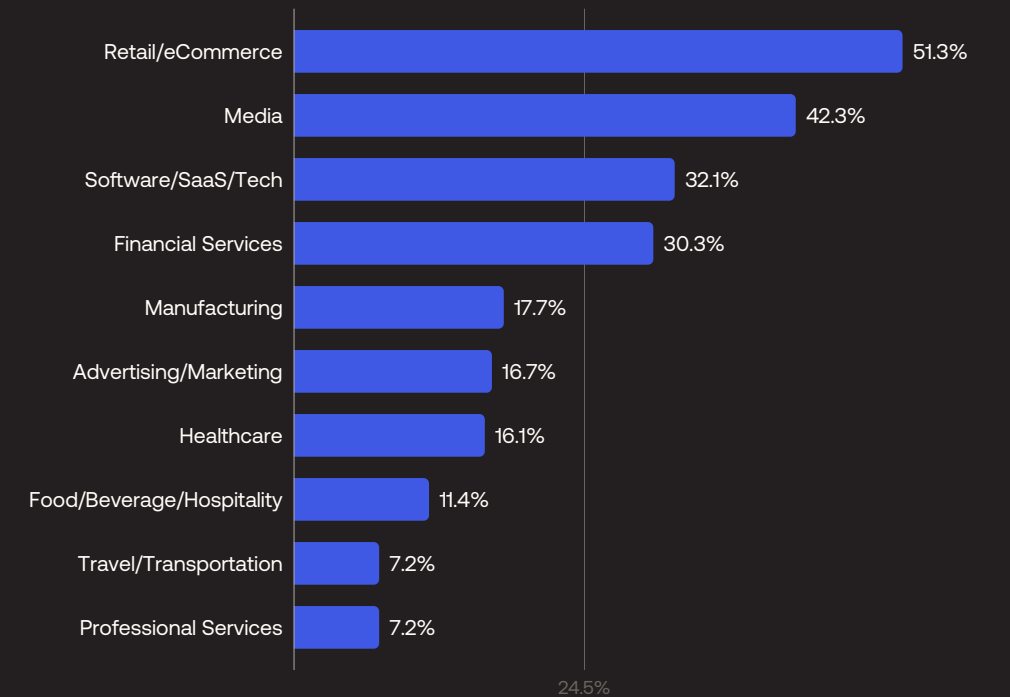
For Retail/eCommerce companies, more than half (51.3%) of all login attempts are attributable to credential stuffing. Clearly, cybercriminals value such accounts — whether to steal loyalty points, to gain unfair access to finite resources, to make purchases with someone else’s money, to acquire payment details, or for some other reason.

Media companies also face a very high proportion of credential stuffing attempts (42.3%), likely for the same reasons examined earlier.

Software/SaaS/Tech companies experience the third-highest proportion (32.1%). In this case, it’s possible that attackers are looking to use the account as a means to access and exfiltrate sensitive information, whether to use directly or to incorporate into a larger attack. For example, a phishing attempt will look more believable if it references project information only available within a trusted service.

Finally, Financial Services organizations also experience a higher-than-average proportion of credential stuffing attacks. Here, an attacker could be acting on many motivations, including stealing personal information to sell or use to commit synthetic identity fraud, and committing financial fraud (e.g., initiating transactions and transfers).

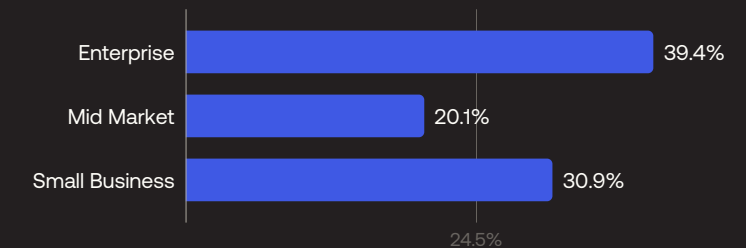
Figure 9: At nearly double the average, Retail/eCommerce companies must grapple with an extraordinarily high proportion of credential stuffing attempts



As was the case with fraudulent signup attempts, we see that small businesses and enterprises experience higher proportions of credential stuffing attempts than do mid-market organizations (Figure 10).

This observation supports the theory suggested earlier that enterprises and small businesses deliver the highest ROI for cybercriminals, while mid-market organizations may be regarded as not being worth the effort.

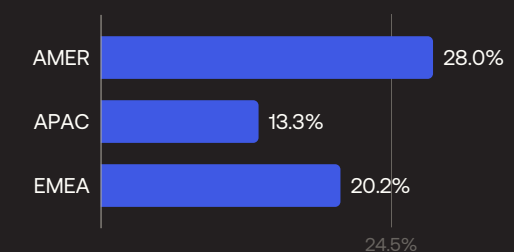
Figure 10: Enterprises and small businesses seem to be more attractive targets than mid-market organizations, possibly because the ROI for cybercriminals is perceived to be higher.



As shown in Figure 11, organizations headquartered in the Americas experience a higher proportion of credential stuffing attempts (28.0%) compared to their counterparts based in APAC (13.3%) or EMEA (20.2%).

A disproportionate number of global Retail/eCommerce, Media, Software/SaaS/Tech, and Financial Services enterprises are based in the Americas; it’s possible that this concentration contributes to the higher proportion of credential stuffing attempts observed in the dataset, both due to the size of the organizations and their familiarity to cybercriminals.

Figure 11: Organizations headquartered in the Americas experience a higher proportion of credential stuffing attempts than those headquartered in APAC or EMEA





Passwords cause problems

When an account holder reuses the same (or similar) passwords on multiple sites, it creates a domino effect in which a single credential pair can be used to breach multiple applications.

Realistically, there's no reason to believe users are going to collectively and spontaneously change their password habits. For example, [Okta's Customer Identity Trends Report 2023](#) found that:

- 33% of survey 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

To make matters worse, active accounts usually make up only a small portion of a user's total number of accounts; many others are forgotten or otherwise not maintained. A breach to any one of these overlooked services may equip a threat actor with a huge volume of user credentials and associated personal data.

And cybercriminals are adept at using this information at scale to compromise accounts that consumers have with other brands. For example, Verizon's [Data Breach Investigation Report \(DBIR\) 2023](#) revealed that 86% of web application breaches involve the use of stolen credentials. Moreover, credentials and personal information (which can be sold, but also can be abused in password recovery flows) are the most common data exfiltrated — continually fueling the attack cycle.

Tomorrow needs to be — and will be — different.

From the perspective of users, the traditional login experience will become a rare exception, and passwords will become an authentication method of last resort — and as reliance on passwords fades, so too will an entire class of Identity attack.

Learn more about this bright future, including what you can do today, in [Authentication after passwords: Maximizing conversions \(and enhancing security\) in the age of convenience](#)

Defensive measures

Again, building on the defensive measures that have already been applied, a number of additional techniques can help to prevent ATOs.

Two straightforward approaches are:

- **Impossible travel:** Detecting when a 'user' attempts to sign in from a geolocation that would be impossible to reach within the time that has passed since the previous successful login.
- **Social login:** In addition to simplifying signups, social login enhances security because a user is more likely to put some effort into protecting their critical social accounts.

More advanced techniques include breached password detection, implementing effective password management (including reset) policies, and — for the highest level of authentication security — requiring strong MFA.

But perhaps the most effective and 'simple' defense against password-based ATOs is to move away from passwords — a prospect that became much more realistic when [Apple, Google, and Microsoft committed to support a common passwordless sign-in standard](#).

Passkeys

Passkeys are FIDO credentials that are discoverable by browsers, or housed within native applications or security keys for passwordless authentication. Based on FIDO Alliance and World Wide Web Consortium (W3C) standards, passkeys replace passwords with cryptographic key pairs and can be accessed (i.e., used) the same way users unlock their mobile devices — typically via biometrics or by entering the device access code.

Passkeys come in two forms: device-bound passkeys and **synced passkeys**.

Each device-bound passkey is tied to a single device, which serves as a possession factor. Device-bound passkeys can be used on FIDO-Certified authenticators and security keys, including those that have achieved security level certification.

Device-bound passkeys have been available for a few years, but some of the same aspects that contribute to strong authentication security (i.e., being tied to a single device) have limited their mainstream adoption.

Synced passkeys, in contrast, are synchronized between a user's devices via a cloud service (e.g., an operating system ecosystem or password manager), creating a user experience that's very familiar to users — arguably a necessary condition for mainstream adoption, especially among consumers.

When a user wants to log in, the site or service asks if they want to use their passkey. To do so, the user simply authenticates on their device (e.g., via biometrics, PIN, or pattern).

From the perspective of the site or service, the passkey validates both a possession factor (i.e., a device permitted to use the synced passkey) and either an inherence factor (when biometrics are used) or a knowledge factor (when the device access code is used). By doing so, synced passkeys meaningfully increase account security for the majority of users — which will help to mitigate password-based ATOs.

Passkeys primer

Mass adoption of passkeys (in either form) by everyday users would represent a major step in the fight against phishing, account takeovers, and other Identity threats.

Learn more in [Passkeys primer: How to improve user experiences and prevent account takeovers by enabling phishing-resistant FIDO authentication](#)

Breached password detection

An unfortunate — but nevertheless very real — aspect of today's threat environment is that entire marketplaces exist to aid adversaries in their actions. For example, threat actors can easily purchase massive lists of breached credentials.

The risks caused by breached credentials can be somewhat managed by leveraging these same credential lists to detect when users are employing a password that has appeared in a breach. Upon detection, an application provider can warn the user and encourage or require some mitigating action on their part (e.g., change the password, enroll in strong MFA).

Fortunately, dedicated password managers and capabilities integrated into web browsers and operating systems are making it easier for users to create, safely store, and easily use longer and more complex passwords, thereby addressing some of the fundamental reasons why users choose and reuse weak passwords; plus, these same solutions often alert users when their credentials appear in leaks, increasing awareness of the risks.

Hopefully, the utility of breached passwords and the threat posed by them will decline as a result of these efforts.



Closing the gap with Credential Guard

It's important to recognize that there can often be a long lag between when breached credentials become available within cybercrime marketplaces and when they appear in threat intelligence feeds, providing attackers with ample time to put them to use.

Credential Guard addresses this gap with a team of experts that infiltrates criminal communities and gains access to exposed data as soon as breaches occur. With this advantage, you can better protect your users and secure your applications by resetting stolen passwords sooner.

Learn more in [Detect Breached Passwords Faster with Auth0 Credential Guard](#)

Effective password policies

In addition to implementing breached password detection, some simple — but effective — ways to enhance Identity security are to:

- Require users to create strong passwords
- Prevent users from switching back to a password they've already used within this application (i.e., preventing password rotation)
- Implement a strong password reset process

Password reset is a necessity for any app — but if your password reset process makes life harder for your customers, you'll be giving them a reason to stop using your service.

For context, Okta's [Customer Identity Trends Report 2023](#) found that:

- 63% of survey 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, customers — especially in B2C — 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.

Good password reset processes do two things:

- 1. They minimize friction for the customer:** It shouldn't take your customer more than a minute to reset their password, and the process should only require information customers are comfortable entering, like email addresses
- 2. They make sure the customer's information is secure:** For example, by providing safeguards against things like multiple failed logins and only sending information via secure channels

Email is most commonly used for password reset because it satisfies both of these criteria: It minimizes friction, as typing in an email address is quick and easy for a customer, and it will protect their information (based upon the presumption that only the customer has access to their inbox).

A single misstep in password reset can ruin your customer's entire experience with your product. These mistakes often come in the form of:

- **Security questions:** Static information — where you went to school, your mother's maiden name, even your pet's name — is easily available via OSINT
- **Passwords in plaintext:** Instead of resetting the password, some sites send the original password back to the customer, which is a massive vulnerability — for a password to be sent in plaintext, it must be stored in plaintext, which means that the chances of attack are increased
- **Error messages:** If an application says whether or not an email address is registered, an attacker could potentially know if a customer has an account — this gives them one more piece of information to use against your customer
- **Requiring unnecessary information:** Security must be balanced with usability — asking customers for a photo ID is a safe practice, but its overall effect on the customer experience is a negative one

(Strong) Multi-factor authentication (MFA)

Protecting accounts through the use of MFA drastically increases the time, effort, and — ultimately — cost of pursuing account takeovers.

However, in practice, MFA's effectiveness as a countermeasure to ATOs is limited by two things:

1. Low rates of adoption by application providers and usage by customers
2. The use of second factors which can be bypassed by threat actors





While a deep-dive into MFA adoption, enrollment, and usage is beyond the scope of this report, we can use the available data to somewhat illuminate the subject.

For example, across the full dataset, the ratio of total password authentication events to valid MFA attempts is roughly 41 — meaning that for every one valid MFA attempt, there are roughly 41 password-based authentications.

We can use this same ratio to determine and compare the relative rates of MFA usage by industry (Figure 12).

Doing so reveals that only three of the 10 most-represented industries appear to have higher-than-average usage of MFA — i.e., have a lower ratio of total password authentications to valid MFA attempts.

In Financial Services, we observe 12 password authentications for each valid MFA event. Manufacturing’s ratio of 24 is double that of Financial Services, but still considerably lower than the 37 of Professional Services.

We can also see that three of the most-represented industries — Food/Beverage/Hospitality (137), Media (155), and Advertising/Marketing (400) — have extremely high ratios, indicating a relative lack of MFA usage.

To satisfy our curiosity, we also looked beyond the 10 most-represented industries and found five others with lower-than-average ratios (Figure 13). Three industries — Legal Services (4), Telecom (6), and Public Sector (6) — are in a class all their own. Considering that all three work with sensitive data or important infrastructure, higher MFA usage is a welcome observation.

So while the ratio examined above is only a proxy metric, it does strongly indicate that certain industries rely upon MFA more than others — in particular, industries that work with sensitive data or systems appear to have higher MFA usage.

However, as Identity defenses in general have hardened and MFA adoption has slowly risen, attackers have focused efforts (Figure 14) on defeating these safeguards.

Figure 12: Highly regulated industries tend to show higher rates of MFA usage with Financial Services and Healthcare both near or below the average (of the 10 industries with the most representation within the dataset)

Ratio of total password authentications to valid MFA attempts (10 most-represented industries, 2023)

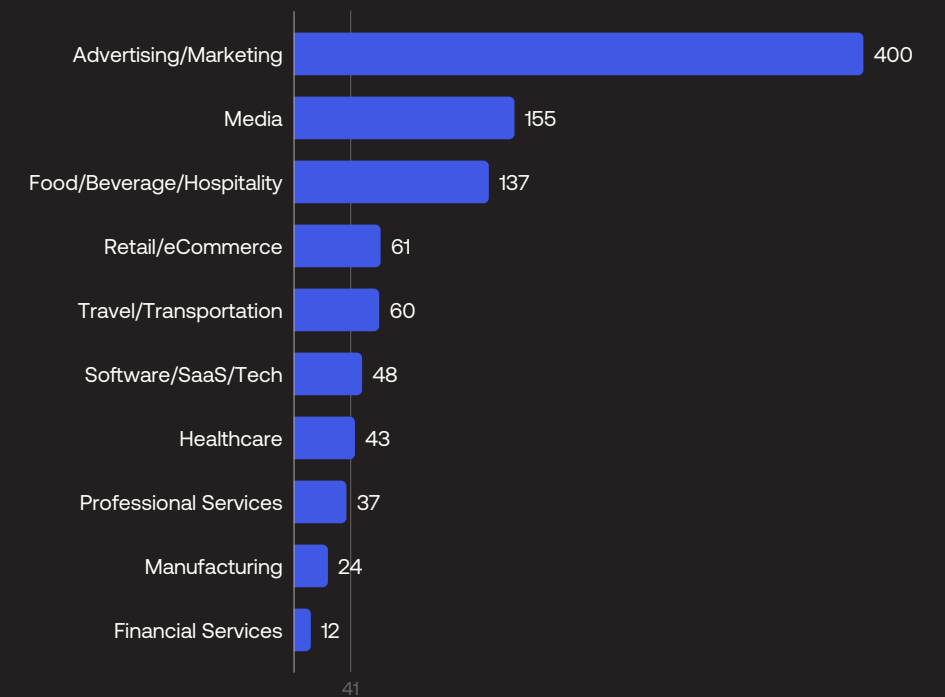
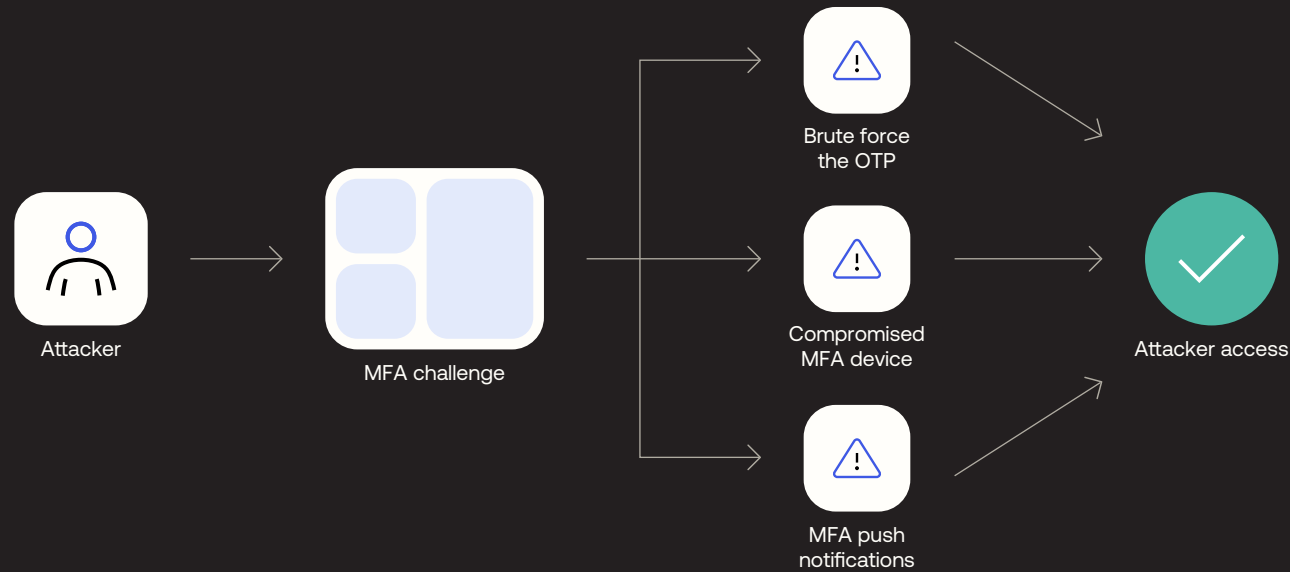


Figure 13: Outside of the 10 most-represented industries, five others have higher-than-average ratios of valid MFA attempts to total password authentications

Ratio of total password authentications to valid MFA attempts (other notable industries, 2023)



Figure 14: Anatomy of common MFA Bypass techniques



For example, several tools are now available that make it easy to attack some of the relatively weaker secondary factors — particularly SMS-delivered one-time passwords (OTPs). The most common attack vector is to apply brute force to create **MFA fatigue** in an attempt to trick or coerce the user into completing the MFA challenge even though they didn't initiate the request; by completing the challenge, the user would inadvertently allow the threat actor to log in.

Plus, threat actors are turning to **SIM swapping** and/or **social engineering** to bypass MFA safeguards.

SIM swapping involves the threat actor convincing the target user's mobile carrier into switching the user's mobile number to a SIM card in the threat actor's possession. Threat actors may rely upon social engineering (e.g., tricking a help desk agent), a malicious insider, or a compromise (i.e., access to the carrier's administrative services) to swap the SIM.

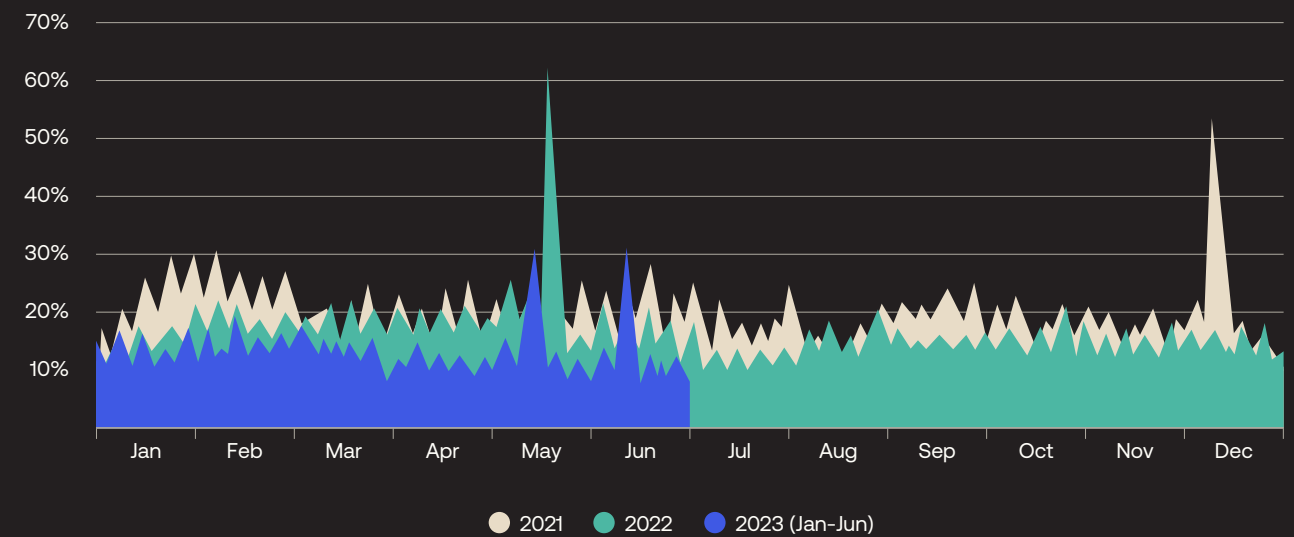
Once the SIM is swapped, any MFA factors that rely on the phone number (e.g., SMS OTP, SMS magic link, voice OTP) can now be completed by the threat actor.

Threat actors may also use social engineering tactics against the application provider, directly. For instance, an attacker equipped with a few pieces of personal information (which is often readily available for purchase or acquired via OSINT) could try to convince a help desk agent to change the account details. Alternatively, the threat actor may even reach out to users directly, in an attempt to trick them into disabling certain account safeguards.

Unfortunately, the cost of executing social engineering campaigns continues to drop, partly due to increased efficiencies (e.g., AI, automation), partly due to massive data breaches and dumps, and partly due to many users' willingness to share information online (e.g., in social media).

For all of these reasons, MFA bypass is a very real risk for today's organizations and their customers. To that point, in the first six months of 2023 (Figure 15), 12.7% of MFA attempts met the technology's MFA bypass criteria. While this proportion represents a decline from 2022 (15.5%) and 2021 (18.1%), the decrease can likely be attributed to a shift in tactics rather than a reduction in the threat itself.

Figure 15: Bypassing MFA is down compared to 2021 and 2022 but it continues to be a focus of threat actors as the cost of executing social engineering continues to drop.





Interestingly, only one of the 10 most-represented industries experienced a higher-than-average proportion of MFA Bypass attempts (Figure 16): Media, at 12.8% (just barely above average, at that). The overall average is buoyed by Public Sector (29.9%) and Entertainment (28.6%) organizations, plus customers for whom we do not have a specific industry assigned.

The threat seems to be particularly prevalent within small businesses (Figure 17), with more than one-fifth (20.3%) of total MFA attempts meeting the criteria to be considered MFA Bypass attempts.

Figure 16: The good news? Some industries still experience average or below-average proportions of MFA Bypass attempts. The Travel/Transportation industry leads the way (among the 10 industries with the most representation within our dataset)

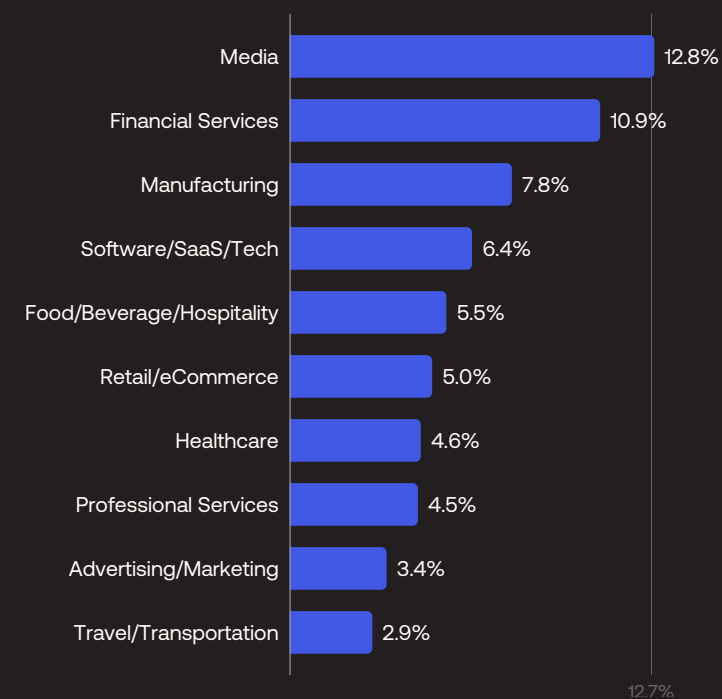
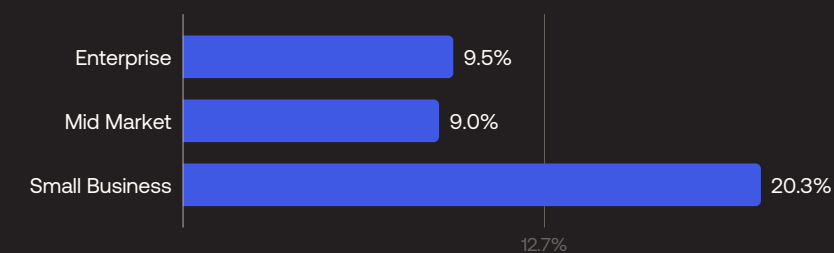


Figure 17: Small businesses appear to endure a higher proportion of MFA Bypass attempts than do enterprises or mid-market organizations





Given the dangerous and rapidly evolving threat landscape, when implementing MFA, it's essential that the solution:

- **Is implemented properly:** Gaps and workarounds (e.g., to support legacy authentication or for administrators to bypass MFA) will be exploited
- **Uses strong secondary factors:** MFA bypass techniques generally target older factors (e.g., those that rely on SMS), and brute-force attacks still focus primarily on knowledge-based authenticators — so using authenticators based on possession or biometric factors can dramatically reduce the likelihood of a brute-force attack being successful

As already noted, technologies that are effective in consumer applications must balance security and usability — and earlier authentication methods often did force a tradeoff between these two characteristics.

However, that tradeoff is increasingly becoming a false choice:

- **Adaptive MFA** is a flexible, extensible MFA policy that can help prevent ATOs without increasing friction for real users. It does so by assessing potential risk during every login transaction, and then prompting the user for additional verification only when necessary

- **New MFA methods are secure and convenient:** MFA methods based on **WebAuthn**-enabled device biometrics (e.g., Apple Face ID, Apple Touch ID, Windows Hello) or WebAuthn-enabled security keys (e.g., YubiKey, Feitian, Titan) simultaneously deliver high security (threat actors hate WebAuthn) and high usability, bringing authentication ever-closer to the ideal solution presented in this report's introduction

While it remains unlikely that consumers at large will adopt dedicated security keys, biometric capabilities are becoming much more common within affordable devices. Enabling users to authenticate using their device biometrics has two benefits:

- It greatly reduces friction during the authentication challenge, boosting user retention and revenue
- It increases security since the flow is not 'phishable' by bad actors ■

Part 3: After the login box

Securing customer identities — and the rights and privileges associated with them — doesn't stop at authentication; rather, efforts should continue for the life of the user's session.



Part 3: After the login box

Attackers value session tokens even more in a passwordless world



After a user authenticates with an application, the browser stores a web cookie; within the web cookie is a session token — a specific block of data that’s generated by the application — which helps keep track of a signed-in user, ensuring they won’t need to sign-in again until the session expires or the user logs out.

If an attacker steals a session cookie and injects it into their browser, they can often access the same session as the legitimate user for as long as the session remains active (a period that varies by application provider).

There are a number of ways in which a session token can be compromised, including:

- **Client-side attacks** (e.g., [T1539](#), [T1185](#)): There are a number of ways to extract a session token from the client, including cross-site scripting (XSS), malicious JavaScript, and malware; notably, many of the most prevalent malware families observed today include ‘infostealer’ modules that have the ability to extract cookies.

- **Adversary-in-the-middle (AiTM) phishing attacks** (e.g., [T1557](#), [T1566](#), [T1539](#)): Using social engineering, attackers direct users to a malicious website that is transparently configured as a reverse HTTP proxy server that relays requests between a targeted user and an impersonated web application; if a user is tricked into signing in to the legitimate web application via one of these malicious sites, then the attacker can access the user’s credentials and the session token returned to the browser. Alternatively, a threat actor reads network traffic (possibly aided by a malicious access point) to observe and steal the session token.

While session hijacking can be scaled somewhat, it is more likely to be used as part of a targeted attack against particular users in high-value organizations.

However, as adoption of passwordless authentication gradually increases, we anticipate that threat actors will invest more effort in session hijacking TTPs.

Sessions for sale

Many stolen session tokens are subsequently sold in cybercrime markets, enabling threat actors who want to compromise an account at a particular organization to simply purchase a suitable token — often for only a few tens of dollars.

As noted below, one way to address this risk is to lower the maximum session time. While doing so doesn’t address the situation in which a user is directly targeted, it can be very effective at combating commodity infostealer malware, as there’s usually a delay between when tokens (and credentials) are harvested and when they are posted to a dark market.

Defensive measures

Three ways to improve session security to guard against session hijacking are to:

- Avoid putting session tokens in the URL
- Use a server-side, secure session manager that generates a new and unpredictable session token after login
- Securely store session tokens and invalidate them after logout
- Shorten the maximum session time

More broadly, application providers should also explore re-authenticating users when circumstances warrant such intervention, as explained below.

Best practices for application session management

Managing application sessions when an Identity Provider (IdP) is involved can be quite challenging — and the first solutions that come to mind are often incomplete.

Learn more in [Best Practices for Application Session Management](#)

Step-up authentication

As we've repeatedly noted, achieving a balance between security and usability is vital for creating a positive user experience.

Step-up authentication empowers application providers to finely tune this balance, in this case by adapting Identity requests to the importance of the resource and the risk level if it were to be exposed.

This tiered approach ensures users (or whomever might be posing as a user) can access some resources with one set of credentials but will be prompted for more credentials (e.g., MFA) when they request access to sensitive resources.

The risk with step-up authentication is in the implementation — [effective implementations](#) require careful planning and consideration.

Continuous authentication

Just because a user passed an authentication challenge initially is no reason to necessarily provide long-lived access.

By continuously monitoring signals (e.g., the user's location, device, apps, consumption patterns, time of day, input behavior, etc.), the authentication system simply checks, whenever needed, to see if the trust is still sufficiently high to allow the user ongoing access.

This "continuous authentication" is extraordinarily powerful, as it enhances both security and the user experience — and the trust that it delivers extends far beyond anything a password by itself can provide.

However, applying continuous authentication within a Customer Identity context would require considerable — and likely ongoing — informed consent from users, plus (potentially) some form of device monitoring. These requirements drastically limit the applications of any continuous authentication solutions to B2B scenarios and highly sensitive B2C use cases (e.g., financial, healthcare). ■



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 organizations leave them unchanged; while it may seem attractive to provision new devices and users with default credentials, it's better to use technologies like OpenID Connect, to go adopt passwordless authentication, or to force users to set a password on first login
- **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

Learn more about Identity management with Auth0 by Okta 

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](https://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.

Afterword

Authorization, the next frontier

There is absolutely no doubt that digital identities are going to become more important in the months, years, and decades to come. Consequently, the ability to manage and secure customer identities will be a foundation of practically every digital interaction.

As we've seen, threats against Customer Identity are pervasive, sophisticated, and evolving — which means that CIAM services must continually anticipate, react, and adapt.

For example, we expect that growing adoption of passkeys will cause cybercriminals to focus more effort on post-authentication TTPs, raising the importance of secure session management, step-up authentication, and continuous authentication.

But authentication is only one aspect of CIAM. Authorization — the process of determining what resources a user can access — is equally important, even if it doesn't receive as much attention. As ever-more rights, information, services, and other privileges are gated by digital identities, authorization will get its turn in the spotlight as an enabler of personalized offerings and as a crucial defense against intrusions and the data breaches that often follow.

Ultimately, securing Customer Identity is about establishing and maintaining the trust that allows real people and real organizations to engage in the countless interactions that make up much of real life.

The stakes — like our commitment — couldn't be higher.

Shiven Ramji

President, Customer Identity Cloud, Okta



Appendices



Appendices

Appendix A: Glossary

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
- **Adaptive multi-factor authentication (Adaptive MFA):** A flexible, extensible MFA policy that can help protect applications from bad actors without increasing friction for real users; the approach assesses potential risk during every login transaction, and then prompts the user for additional verification if appropriate
- **Authentication:** The confirmation of a digital identity (i.e., how apps identify who users are)
- **Authorization:** The process of determining what resources a user can access (i.e., 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
- **Device-bound passkey:** A passkey that is bound to a single specific device, thereby providing proof of a possession factor
- **Digital Identity:** The set of attributes that define a particular user in the context of an application
- **Entity:** A singular and identifiable object, which exists independent of changes to its attributes; in the CIAM context, an entity is typically either a user, device, or computing resource (e.g., a system or application)
- **FIDO:** Meaning “Fast Identity Online”; often used as the short form of the FIDO Alliance, an open industry association with a focused mission to develop and champion authentication standards to help reduce the world’s over-reliance on passwords
- **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
- **Intrusion:** A security event (or a combination of multiple security events) in which an unauthorized user gains access to a system or system resource
- **Magic link:** A link generated by the authentication API, which is sent to the user; upon clicking the link, the user is logged in directly (a magic link is similar in function to a user receiving an email with an OTP, returning to an application, and entering the OTP — but without having to actually perform those steps)
- **MFA fatigue:** A technique used by attackers to flood a user with MFA notifications in the hope they will accept/approve, thereby enabling the attacker to gain entry to an account or device
- **Multi-factor authentication (MFA):** A user authentication method that requires more than one type of factor (e.g., biometric, one-time passcode, authenticator application, etc.)
- **One-time passcode/password (OTP):** A sequence of numeric or alphanumeric characters generated by the authentication API that will authenticate a user for a single login or transaction
- **Open-source intelligence (OSINT):** The collection, analysis, and dissemination of information that is publicly available and legally accessible (per [SANS](#))
- **Passkey:** FIDO credentials that are discoverable by browsers, or housed within native applications or security keys for passwordless authentication
- **Passwordless:** Passwordless authentication (often shortened to “passwordless”) refers to any mechanism that authenticates a user without requiring them to enter their password
- **Phishing:** A social engineering technique that typically uses deception, pressure, or manipulation to trick users into sharing sensitive information
- **SIM swapping:** A technique that allows an attacker to gain control of a user’s mobile phone number by convincing the target user’s mobile carrier into switching the user’s mobile number to a SIM card in the threat actor’s possession
- **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 engineering:** An umbrella term encompassing all tactics and techniques aimed at tricking a target into revealing sensitive information or performing an action on the threat actor’s behalf
- **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
- **Spear phishing:** A highly targeted form of phishing (e.g., an individual or an organization) that often includes information and details of particular relevance that are presumed by the target not to be widely known
- **Step-up authentication:** An authentication approach intended to strike a fine balance between security and friction by allowing users to access some resources with one set of credentials — but which prompt them for more credentials when they request access to sensitive resources
- **Synced passkey:** A passkey that can be securely shared across/between multiple devices (e.g., within an operating system ecosystem or via a password manager)
- **WebAuthn:** Short form of Web Authentication JavaScript API standard, part of the FIDO2 specification

Appendices

Appendix B: Methodology

This report is based on data from the Okta Customer Identity Cloud, powered by Auth0, which provides CIAM functionality for thousands of organizations large and small around the world.

More specifically, the report sums daily event logs into numerators (e.g., fraudulent signup events) and denominators (e.g., total signup events), allowing for the meaningful normalization of threat trends and controlling for ongoing changes in the Customer Identity Cloud customer composition.

Where such information is available, event data is joined with a tenant's industry (self-selected), size (e.g., Small Business, Mid-Market, Enterprise), and headquarter region, before being anonymously aggregated.

Because this report is based on real production deployments, it captures the actual activity on the Customer Identity Cloud, and therefore is heavily shaped both by the products and features each customer has enabled (as well as their configurations), and by the evolving capabilities of these products and features.

To determine which 10 industries have the most representation on the Customer Identity Cloud, we ranked each industry by four factors (over the first six months of 2023):

- Number of tenants
- Total signup events
- Total password authentication events
- Total MFA attempts

We considered the 10 industries with the highest average ranking to have the most representation.

Subset analysis is dependent upon attributes that may not be available for all customers/tenants (e.g., industry, size, HQ location). This means that charts which show a global aggregation based upon such attributes do not include all tenants. For example, while Figure 3 is based upon data from all tenants, Figure 6 only includes tenants for whom:

- We have an associated HQ country
- That HQ country is located in one of the AMER, APAC, or EMEA regions.

This means Figure 6 does not include data from tenants for whom we lack an HQ country or whose HQ country falls outside of those three regions (e.g., Africa).

In one extreme case, this subset-effect created a scenario in which all three major regions showed below-average (i.e., below the global average) proportions of MFA Bypass attempts. The simple explanation is that customers either based outside of the three main regions or for whom we lack HQ data altogether also contribute to the global average, and — in this case — pushed it higher than that experienced by customers known to be based in AMER, APAC, or EMEA.



Appendices

Appendix C: Industry-based summaries

The following subsections provide additional context for the 10 industries with the most representation within the 2023 dataset:

Advertising/Marketing

Dedicated to creating, promoting, and distributing campaigns that inform and engage audiences to support products or services

Financial Services

Includes banking, insurance, wealth management, and other services designed to manage and distribute capital

Food/Beverage/Hospitality

Includes the production and distribution of, and services related to, food and beverages, as well as leisure activities and accommodations, such as hotels and restaurants

Healthcare

Includes healthcare providers, payers (such as medical insurances), pharmaceuticals, and healthcare technology

Manufacturing

Includes the production of physical goods, ranging from consumer electronics to automobiles

Media

Includes organizations that create, distribute, and broadcast content such as news, entertainment, and advertising

Professional Services

Includes a wide range of services to support business needs, such as legal, consulting, accounting, and marketing

Retail/eCommerce

Includes organizations that sell and distribute products and services to consumers through physical stores or digital platforms

Software/SaaS/Tech

Centered on the development, distribution, and support of software, including software-as-a-service (SaaS) and technology

Travel/Transportation

Includes airlines, railways, hotels, travel agencies, and related services specializing in the movement of people and goods



Table 2: Advertising/Marketing

Summary of Identity threat trends against Advertising/Marketing organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	1.4%	1.5%	1.0%
Credential Stuffing Attempts	2.7%	4.9%	16.9%
MFA Bypass Attempts	17.6%	4.1%	3.4%

Figure 18: 30-month daily view of Identity threats against Advertising/Marketing organizations

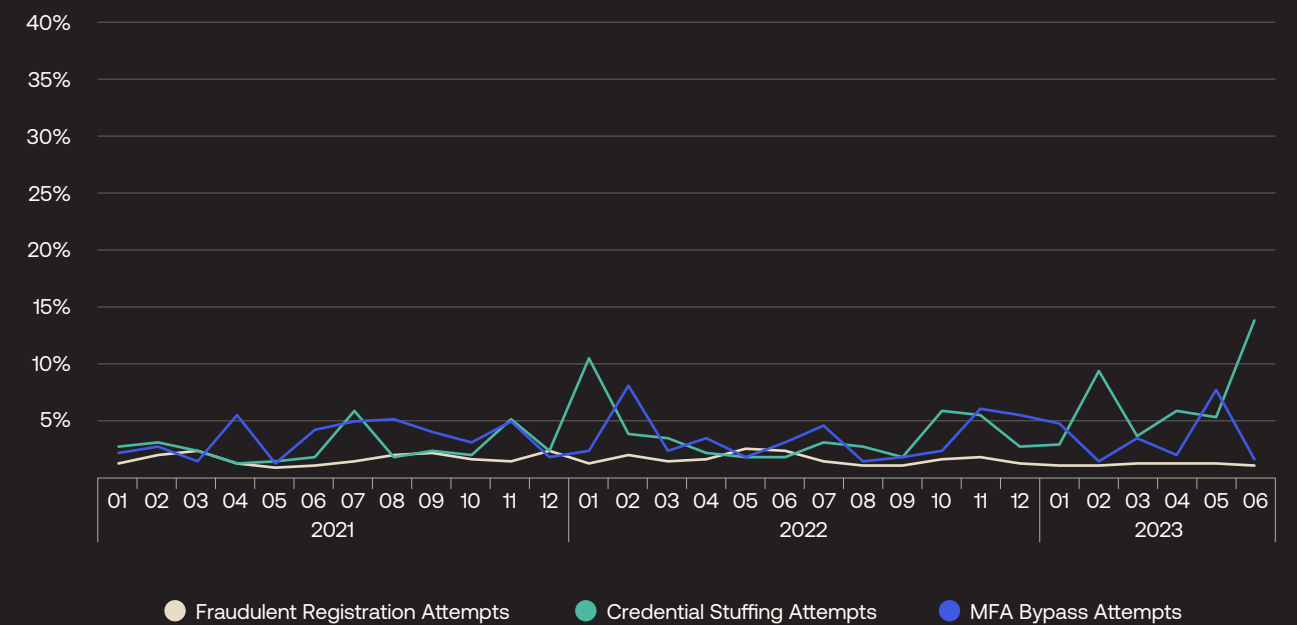


Table 3: Financial Services

Summary of Identity threat trends against Financial Services organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	23.4%	50.8%	28.8%
Credential Stuffing Attempts	46.6%	41.8%	30.3%
MFA Bypass Attempts	3.7%	4.8%	10.9%

Figure 19: 30-month daily view of Identity threats against Financial Services organizations

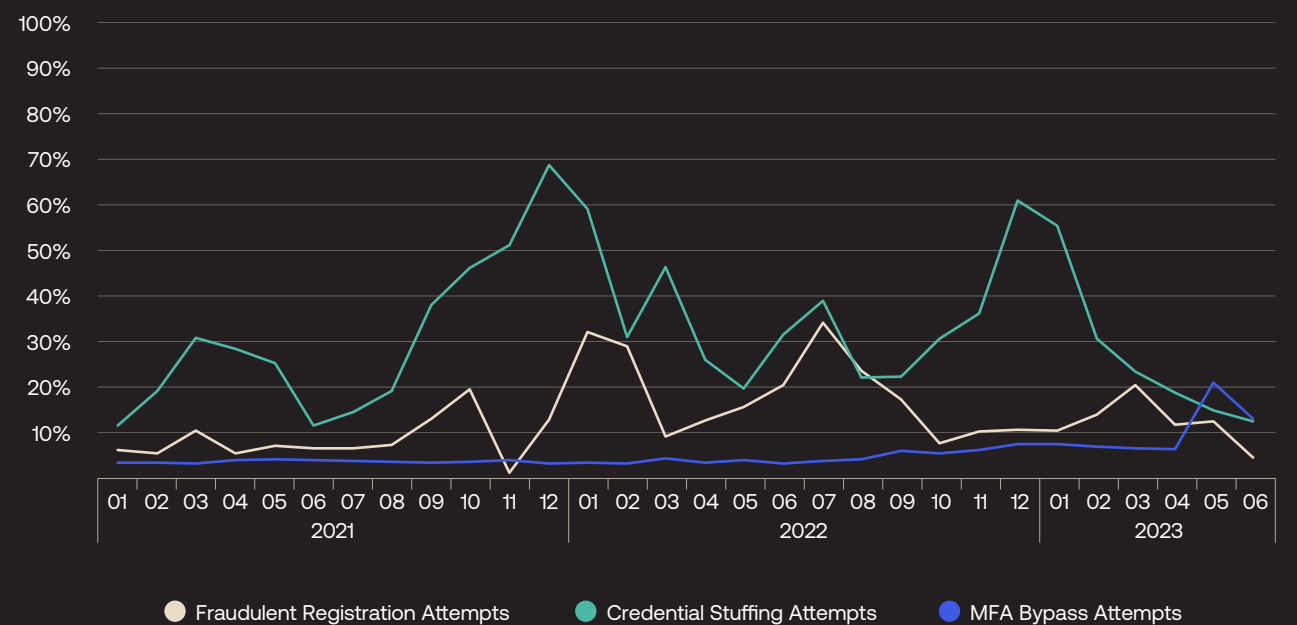


Table 4: Food/Beverage/Hospitality

Summary of Identity threat trends against Food/Beverage/Hospitality organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	3.3%	17.8%	9.0%
Credential Stuffing Attempts	23.6%	21.5%	11.4%
MFA Bypass Attempts	8.3%	9.2%	5.5%

Table 5: Healthcare

Summary of Identity threat trends against Healthcare organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	1.9%	2.8%	6.3%
Credential Stuffing Attempts	4.5%	3.3%	16.1%
MFA Bypass Attempts	6.0%	9.0%	4.6%

Figure 20: 30-month daily view of Identity threats against Food/Beverage/Hospitality organizations

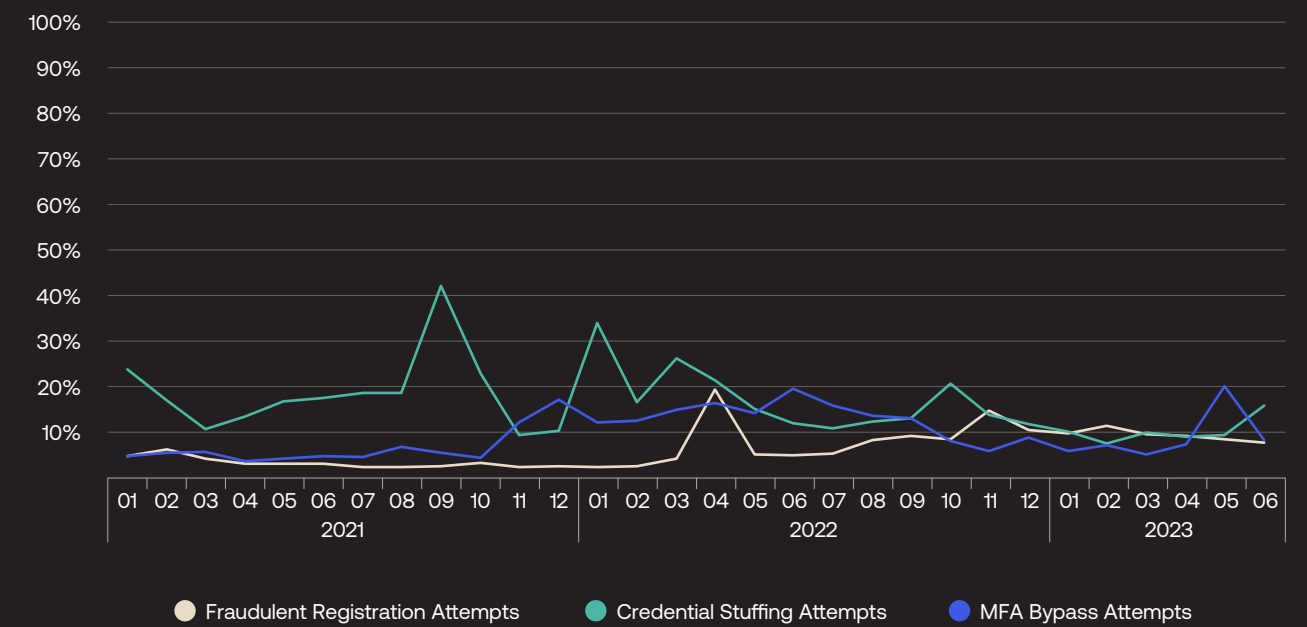


Figure 21: 30-month daily view of Identity threats against Healthcare organizations

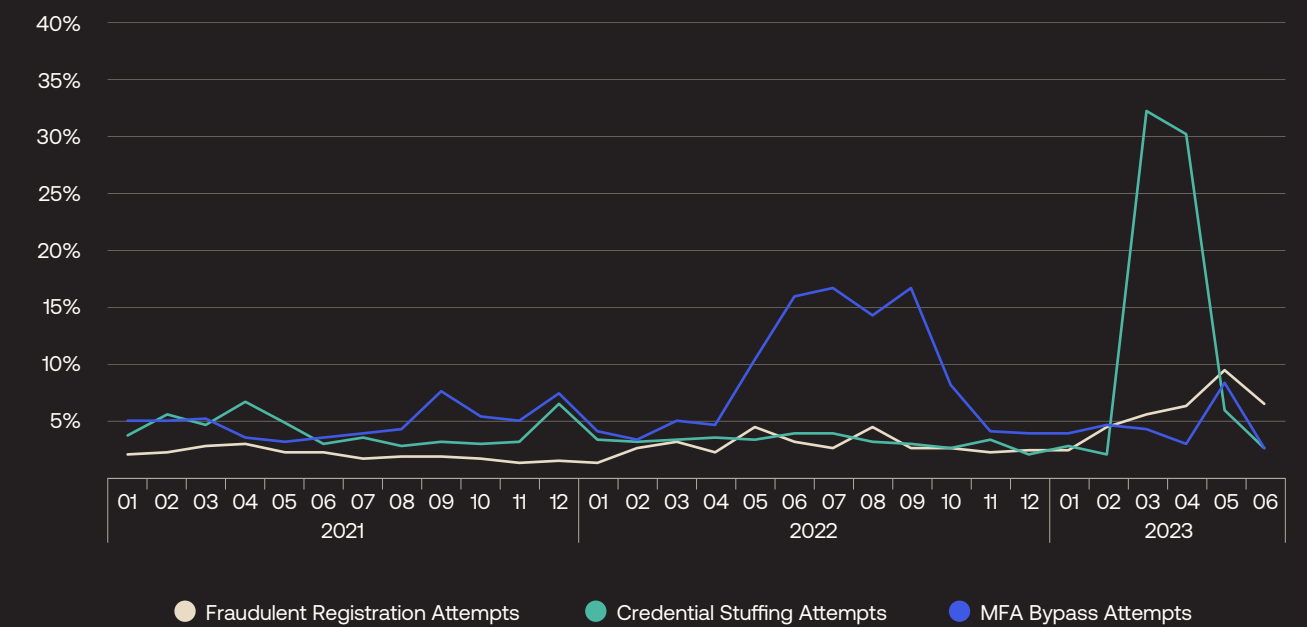


Table 6: Manufacturing

Summary of Identity threat trends against Manufacturing organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	14.3%	17.8%	25.1%
Credential Stuffing Attempts	45.9%	18.4%	17.7%
MFA Bypass Attempts	6.5%	10.0%	7.8%

Table 7: Media

Summary of Identity threat trends against Media organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	9.0%	15.7%	28.4%
Credential Stuffing Attempts	22.7%	17.9%	42.3%
MFA Bypass Attempts	27.4%	25.1%	12.8%

Figure 22: 30-month daily view of Identity threats against Manufacturing organizations

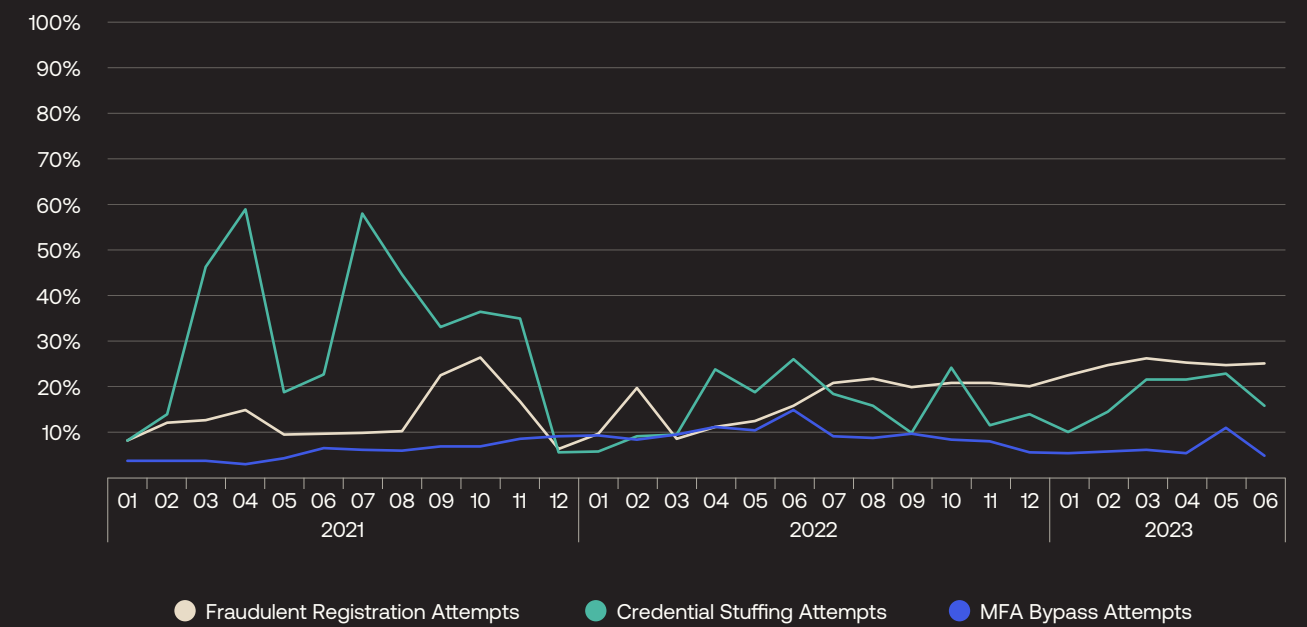


Figure 23: 30-month daily view of Identity threats against Media organizations

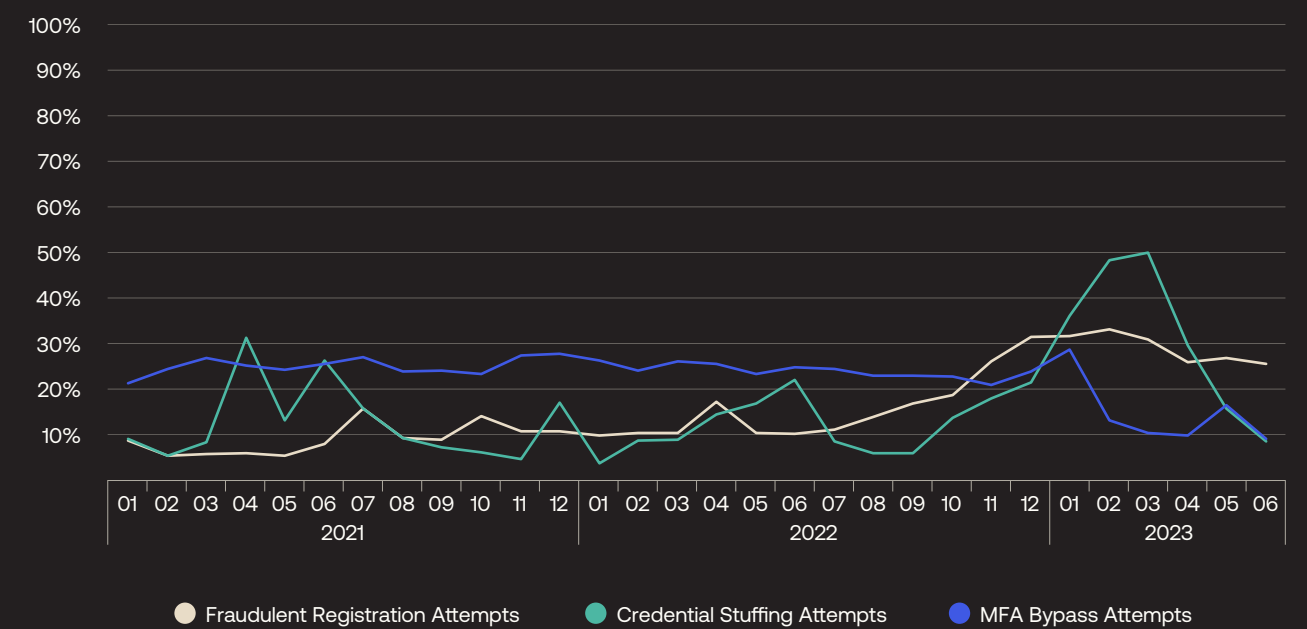


Table 8: Professional Services

Summary of Identity threat trends against Professional Services organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	5.9%	6.1%	13.4%
Credential Stuffing Attempts	7.3%	4.8%	7.2%
MFA Bypass Attempts	13.1%	6.7%	4.5%

Table 9: Retail/eCommerce

Summary of Identity threat trends against Retail/eCommerce organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	2.0%	3.6%	9.3%
Credential Stuffing Attempts	55.6%	56.8%	51.3%
MFA Bypass Attempts	5.7%	5.3%	5.0%

Figure 24: 30-month daily view of Identity threats against Professional Services organizations

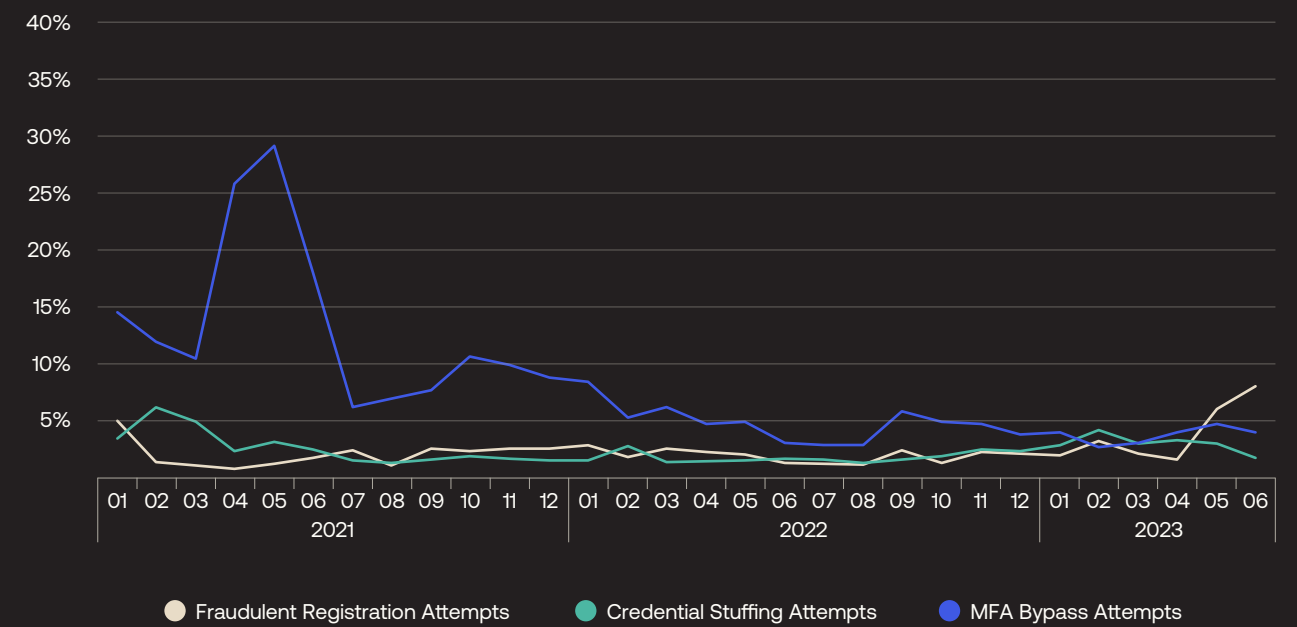


Figure 25: 30-month daily view of Identity threats against Retail/eCommerce organizations

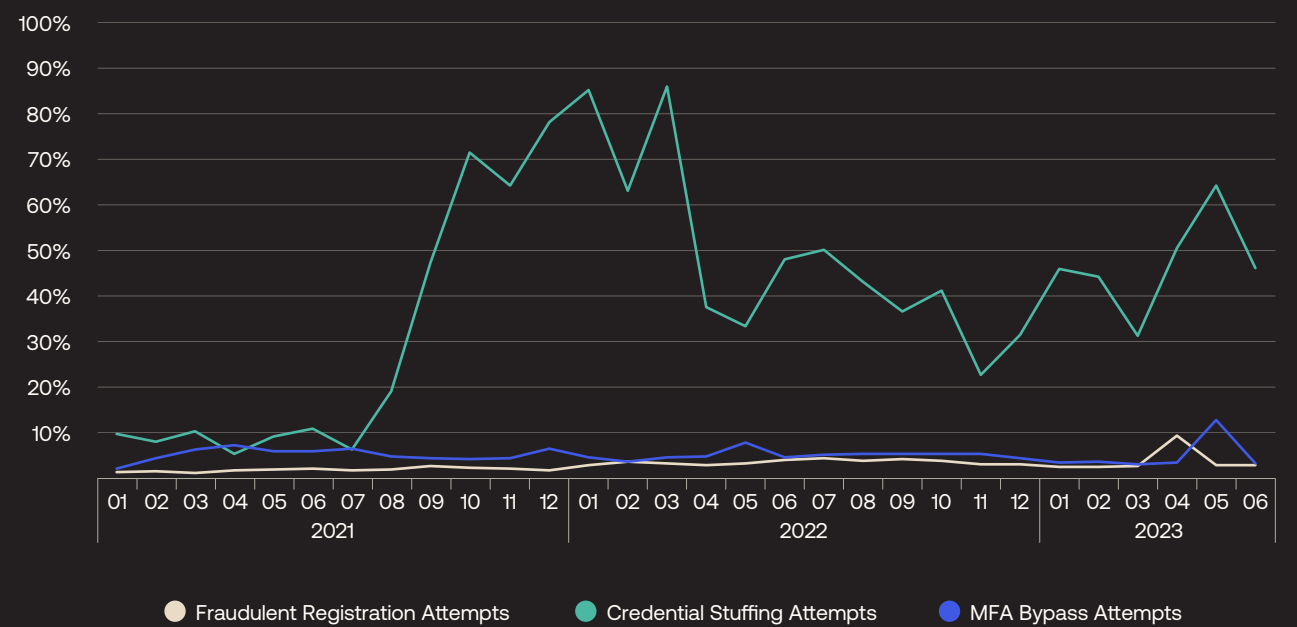


Table 10: Software/SaaS/Tech

Summary of Identity threat trends against Software/SaaS/Tech organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	54.9%	26.1%	24.0%
Credential Stuffing Attempts	53.6%	34.5%	32.1%
MFA Bypass Attempts	37.5%	21.6%	6.4%

Table 11: Travel/Transportation

Summary of Identity threat trends against Travel/Transportation organizations

	2021	2022	1H2023
Fraudulent Registration Attempts	5.1%	13.7%	9.7%
Credential Stuffing Attempts	27.4%	19.0%	7.2%
MFA Bypass Attempts	6.9%	3.0%	2.9%

Figure 26: 30-month daily view of Identity threats against Software/SaaS/Tech organizations

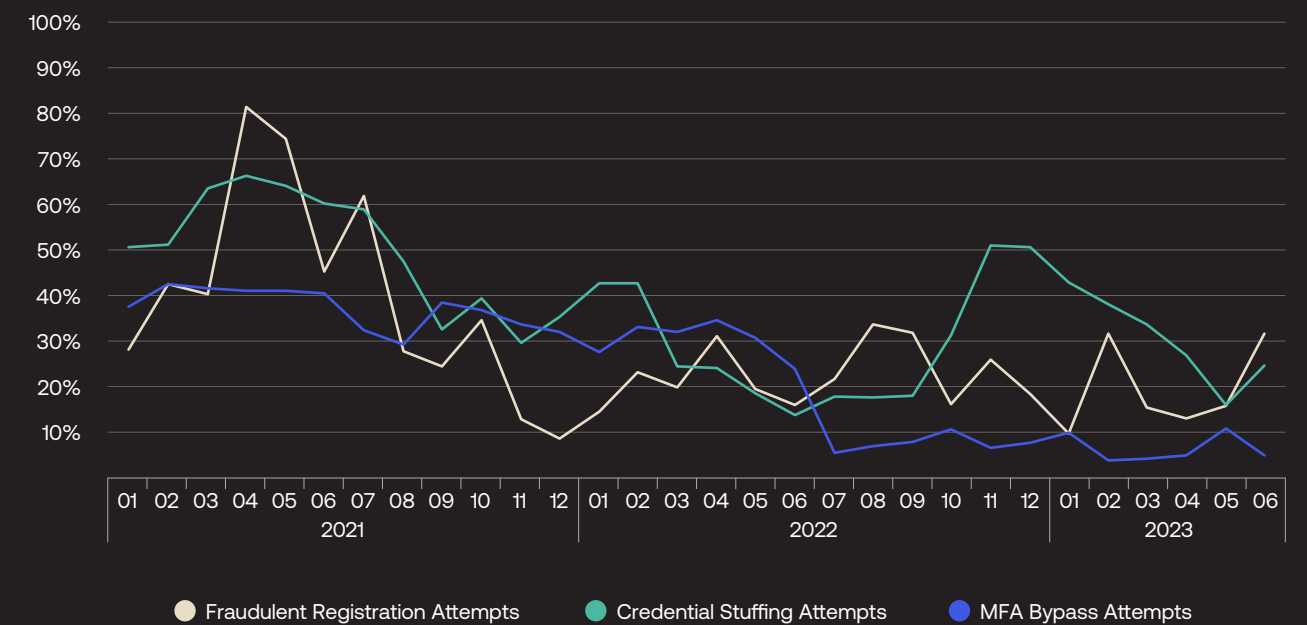
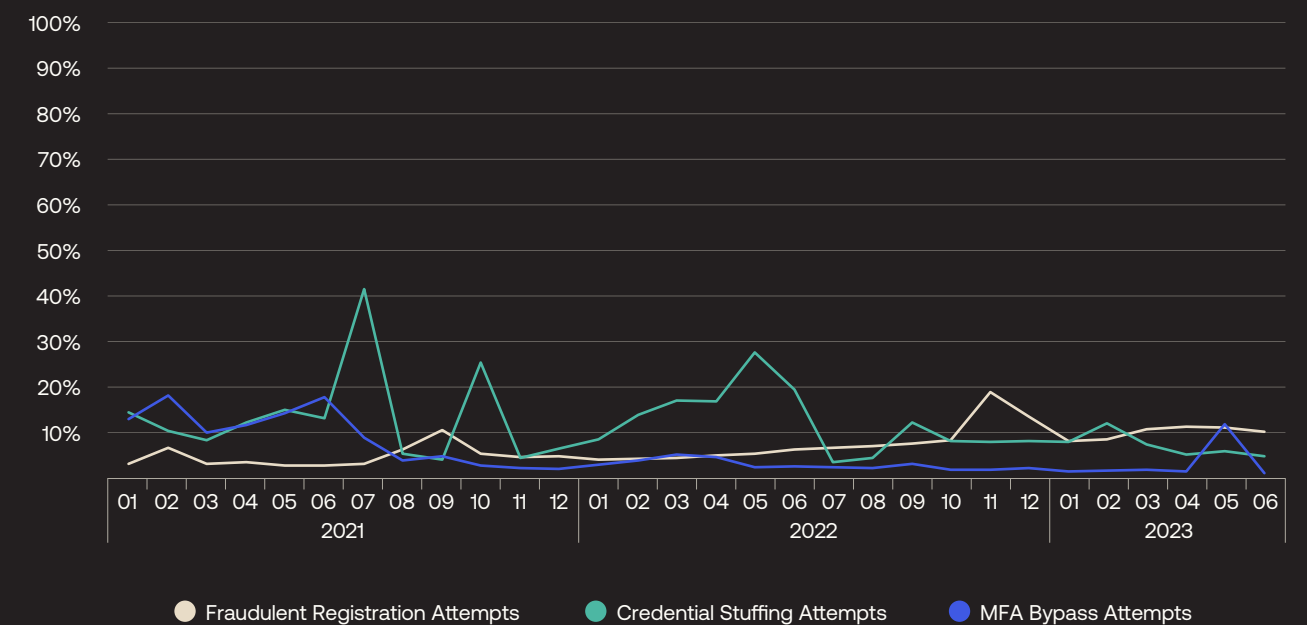


Figure 27: 30-month daily view of Identity threats against Travel/Transportation organizations



Appendices

Appendix D: Size-based summaries

The following subsections provide additional context for small businesses, mid-market organizations, and enterprises.

Table 12: Small Business

Summary of Identity threat trends against the small business segment

	2021	2022	1H2023
Fraudulent Registration Attempts	65.1%	44.6%	19.4%
Credential Stuffing Attempts	54.0%	35.7%	30.9%
MFA Bypass Attempts	9.1%	25.0%	20.3%



Figure 28: 30-month daily view of Identity threats against the small business segment

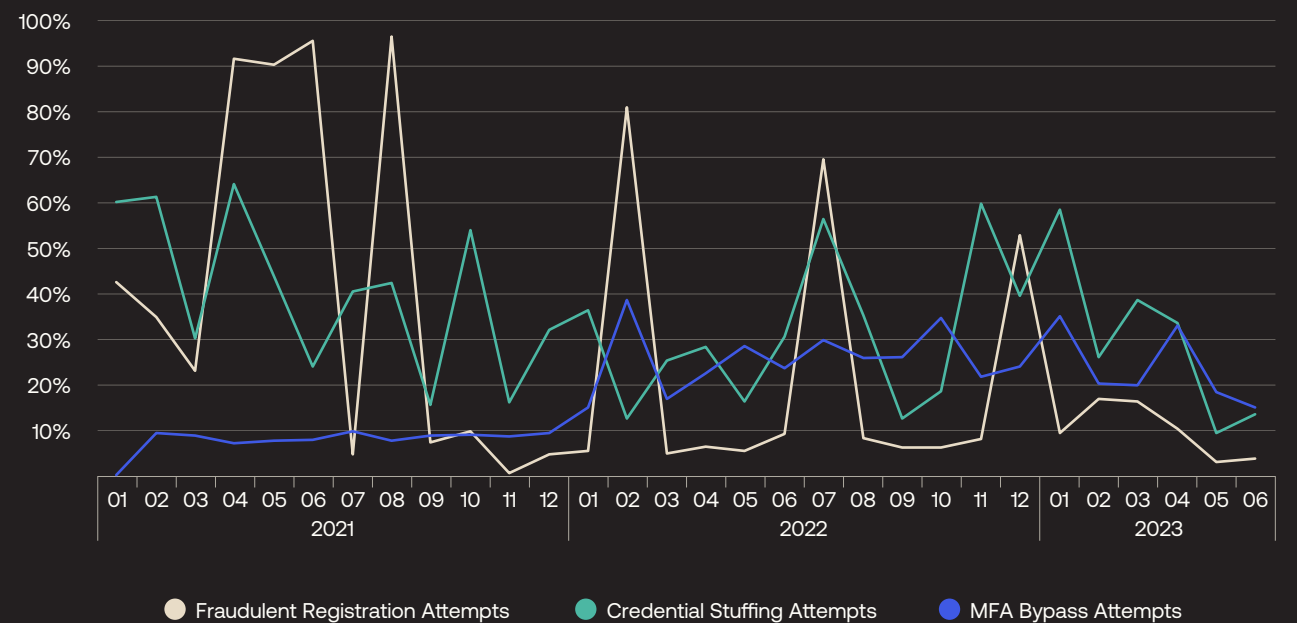


Table 13: Mid-Market

Summary of Identity threat trends against the mid-market segment

	2021	2022	1H2023
Fraudulent Registration Attempts	39.9%	6.0%	12.6%
Credential Stuffing Attempts	32.1%	30.5%	20.1%
MFA Bypass Attempts	4.4%	6.2%	9.0%

Figure 29: 30-month daily view of Identity threats against the mid-market segment

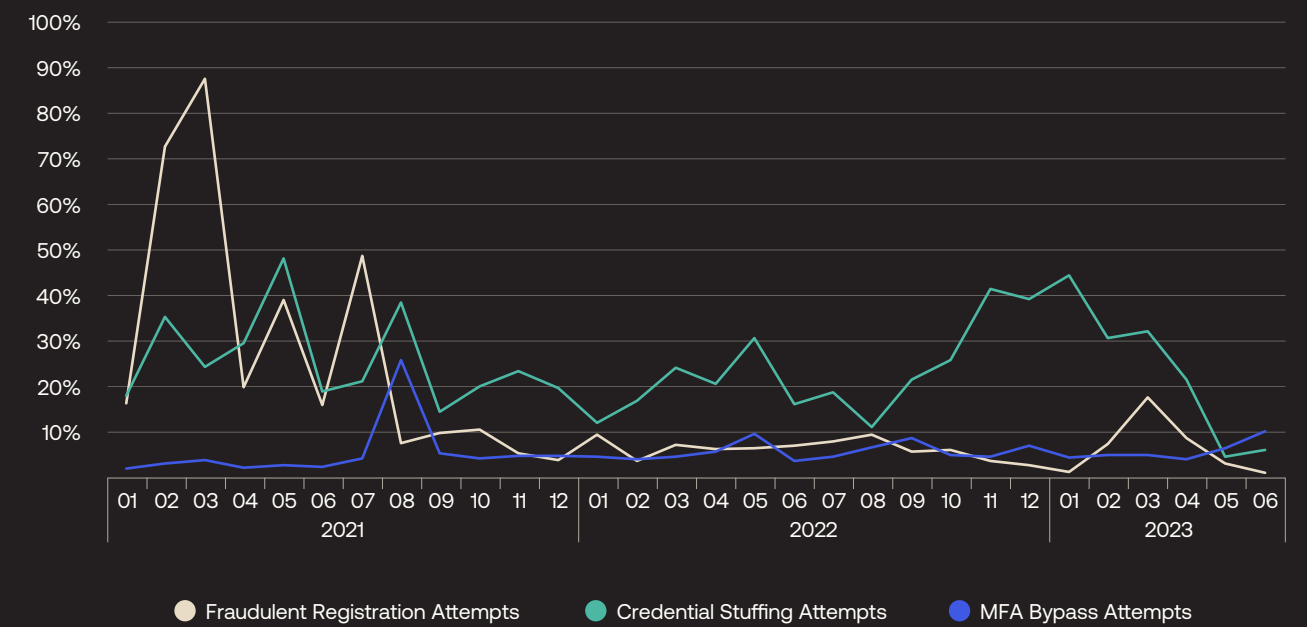
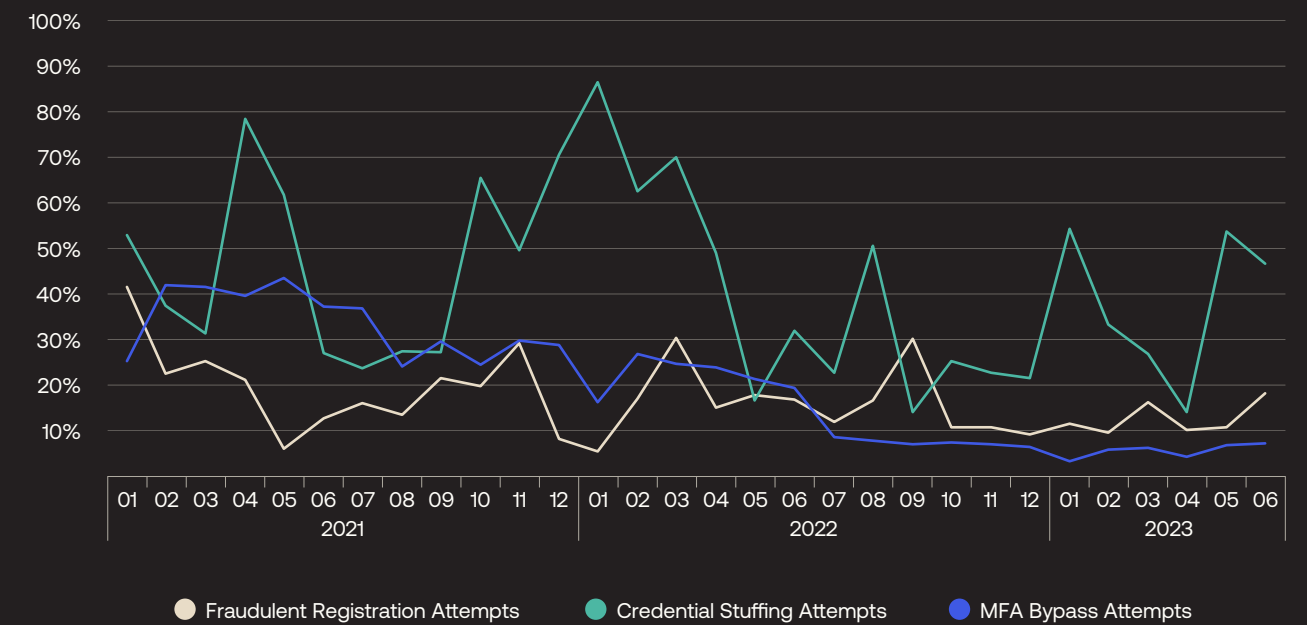


Table 14: Enterprise

Summary of Identity threat trends against the enterprise segment

	2021	2022	1H2023
Fraudulent Registration Attempts	16.2%	20.7%	19.9%
Credential Stuffing Attempts	50.6%	44.0%	39.4%
MFA Bypass Attempts	32.3%	16.4%	9.5%

Figure 30: 30-month daily view of Identity threats against the enterprise segment



Appendices

Appendix E: Region-based summaries

The following subsections provide additional context for geography-oriented analysis.

Note: As the area of focus tightens, the sample size of the relevant dataset also shrinks, which can result in more frequent and higher-amplitude short-term fluctuations.



Table 15: The Americas

Potentially includes any countries within the United States Federal Aviation Authority's [listing of countries in the Western Hemisphere](#).

Summary of Identity threat trends against organizations headquartered in the Americas

	2021	2022	1H2023
Fraudulent Registration Attempts	35.8%	14.7%	9.4%
Credential Stuffing Attempts	48.1%	43.8%	28.0%
MFA Bypass Attempts	6.9%	11.0%	12.0%

Table 16: Latin America

Countries potentially included: Argentina, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, French Guiana, Guatemala, Guyana, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Suriname, Uruguay, and Venezuela.

Summary of Identity threat trends against organizations headquartered in Latin America

	2021	2022	1H2023
Fraudulent Registration Attempts	15.8%	13.7%	5.7%
Credential Stuffing Attempts	59.0%	31.3%	17.6%
MFA Bypass Attempts	5.0%	4.8%	10.7%

Figure 31: 30-month daily view of Identity threats against organizations headquartered in the Americas

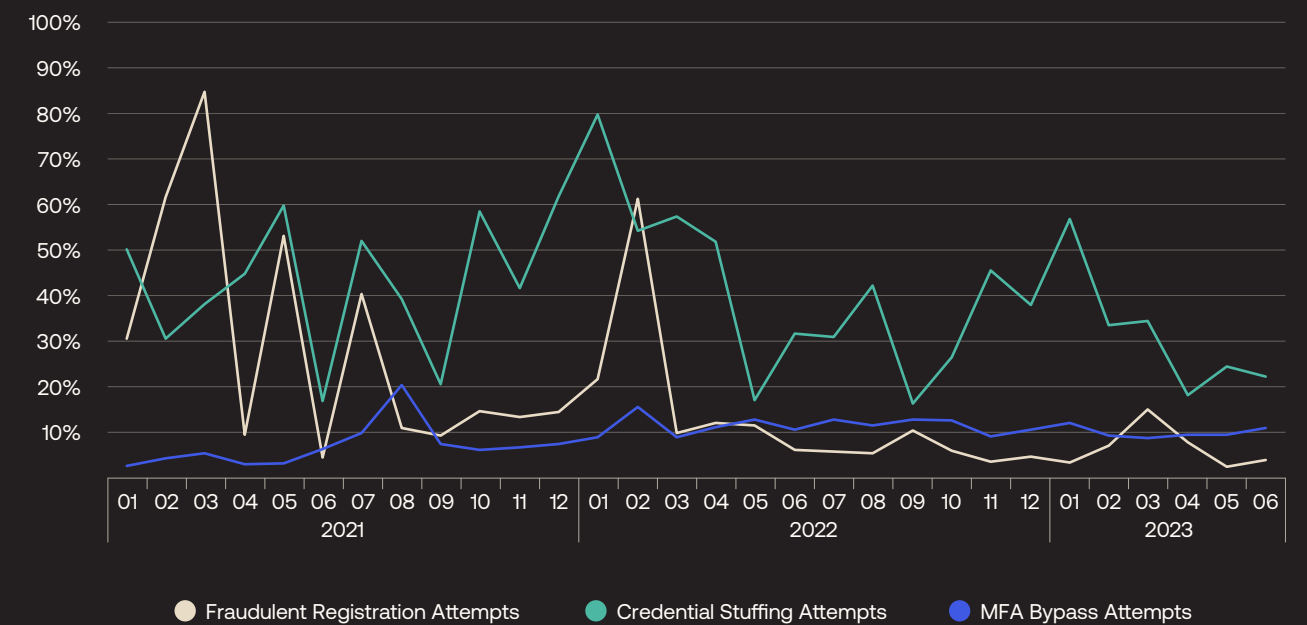


Figure 32: 30-month daily view of Identity threats against organizations headquartered in Latin America

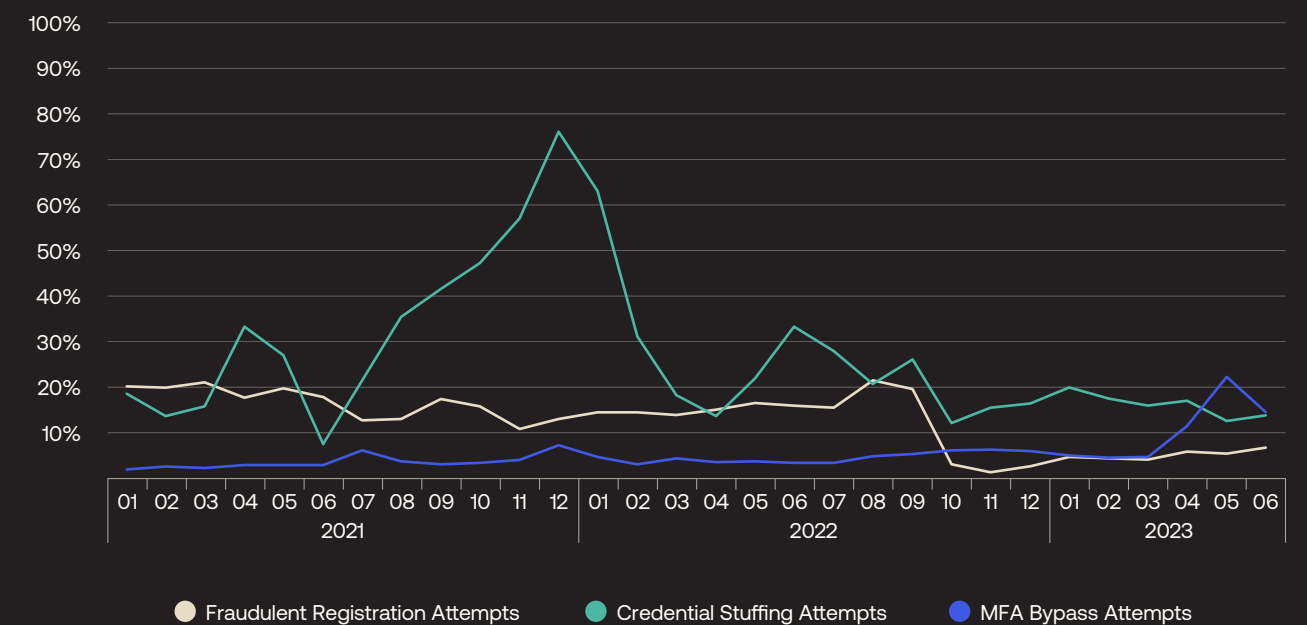


Table 17: United States & Canada

Summary of Identity threat trends against organizations headquartered in the United States or Canada

	2021	2022	1H2023
Fraudulent Registration Attempts	37.1%	14.8%	9.5%
Credential Stuffing Attempts	46.1%	45.1%	28.5%
MFA Bypass Attempts	7.5%	14.1%	12.4%

Table 18: Europe, Middle East, and Africa

Potentially includes any countries within the United States Federal Aviation Authority's [listing of countries in Africa, Europe, and the Middle East](#).

Summary of Identity threat trends against organizations headquartered in Europe, the Middle East, or Africa

	2021	2022	1H2023
Fraudulent Registration Attempts	18.1%	20.5%	8.1%
Credential Stuffing Attempts	26.4%	14.1%	20.2%
MFA Bypass Attempts	34.8%	20.3%	7.6%

Figure 33: 30-month daily view of Identity threats against organizations headquartered in the United States or Canada

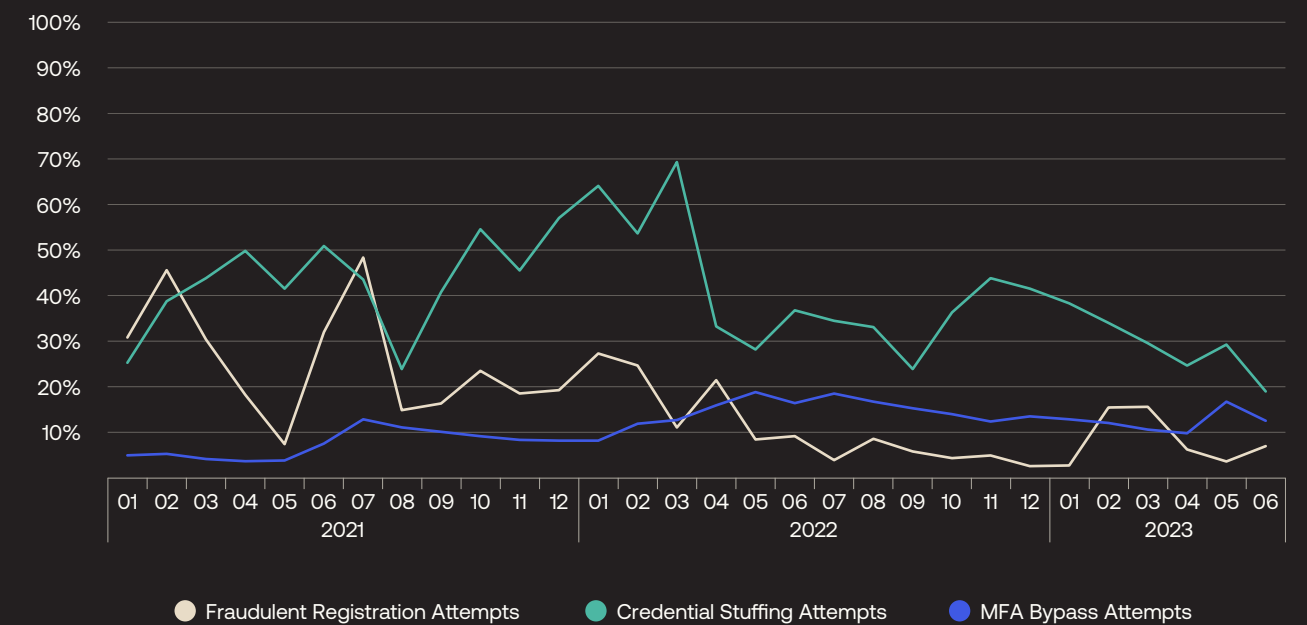


Figure 34: 30-month daily view of Identity threats against organizations headquartered in Europe, the Middle East, or Africa

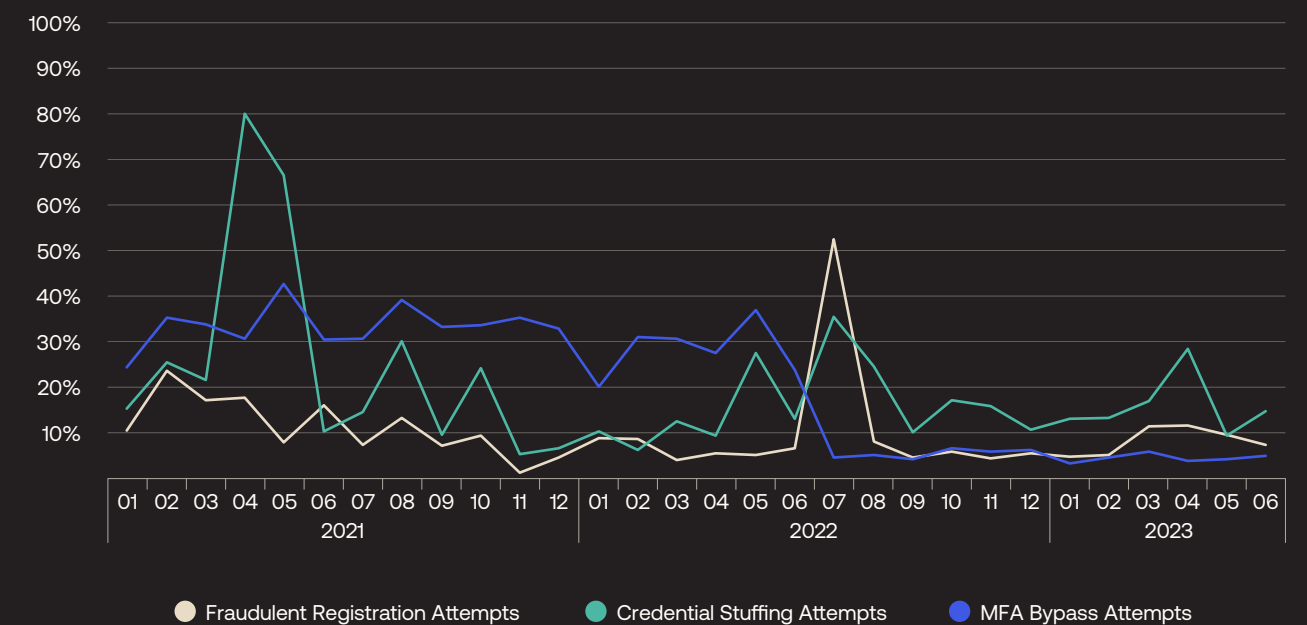


Table 19: Nordics

Countries potentially included: Denmark, Finland, Iceland, Norway, Sweden, and Greenland.

Summary of Identity threat trends against organizations headquartered in the Nordics

	2021	2022	1H2023
Fraudulent Registration Attempts	45.4%	14.9%	5.2%
Credential Stuffing Attempts	15.0%	5.2%	12.5%
MFA Bypass Attempts	6.0%	2.9%	4.1%

Table 20: Southern Europe

Countries potentially included: Albania, Andorra, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Turkey, Gibraltar, Greece, Italy, Kosovo, Malta, Montenegro, North Macedonia, Portugal, San Marino, Serbia, Slovenia, Spain, and Vatican City.

Summary of Identity threat trends against organizations headquartered in Southern Europe

	2021	2022	1H2023
Fraudulent Registration Attempts	11.7%	15.2%	24.8%
Credential Stuffing Attempts	18.1%	14.9%	10.9%
MFA Bypass Attempts	5.2%	4.7%	5.5%

Figure 35: 30-month daily view of Identity threats against organizations headquartered in the Nordics

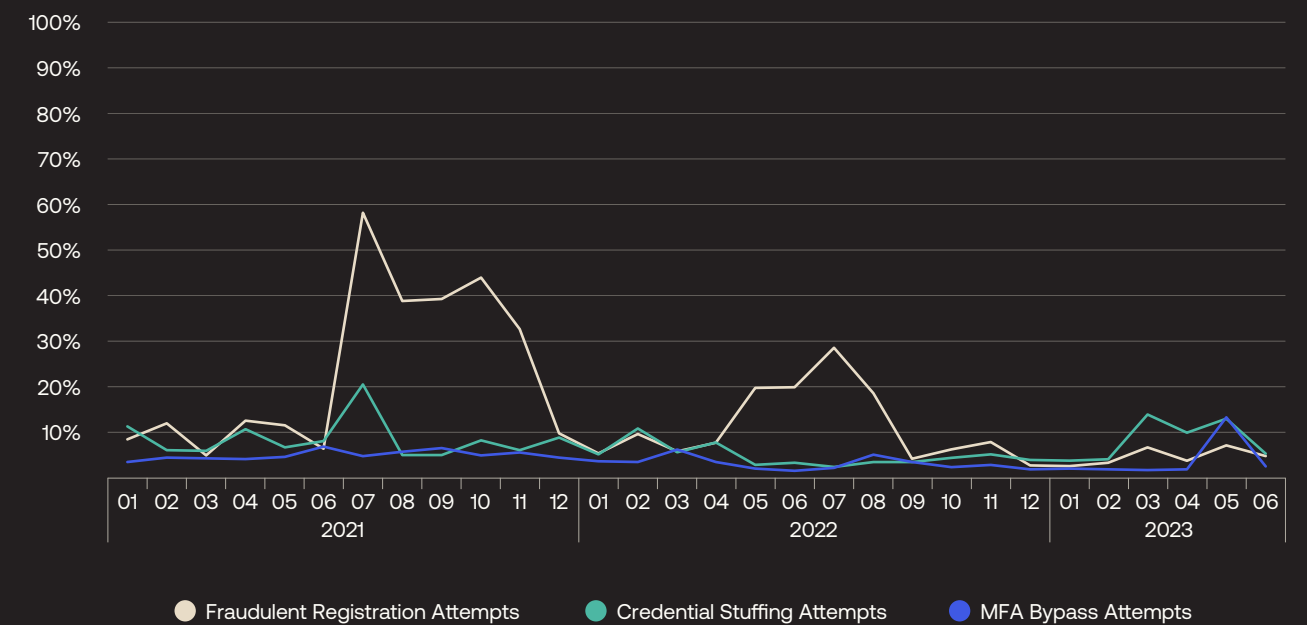


Figure 36: 30-month daily view of Identity threats against organizations headquartered in Southern Europe

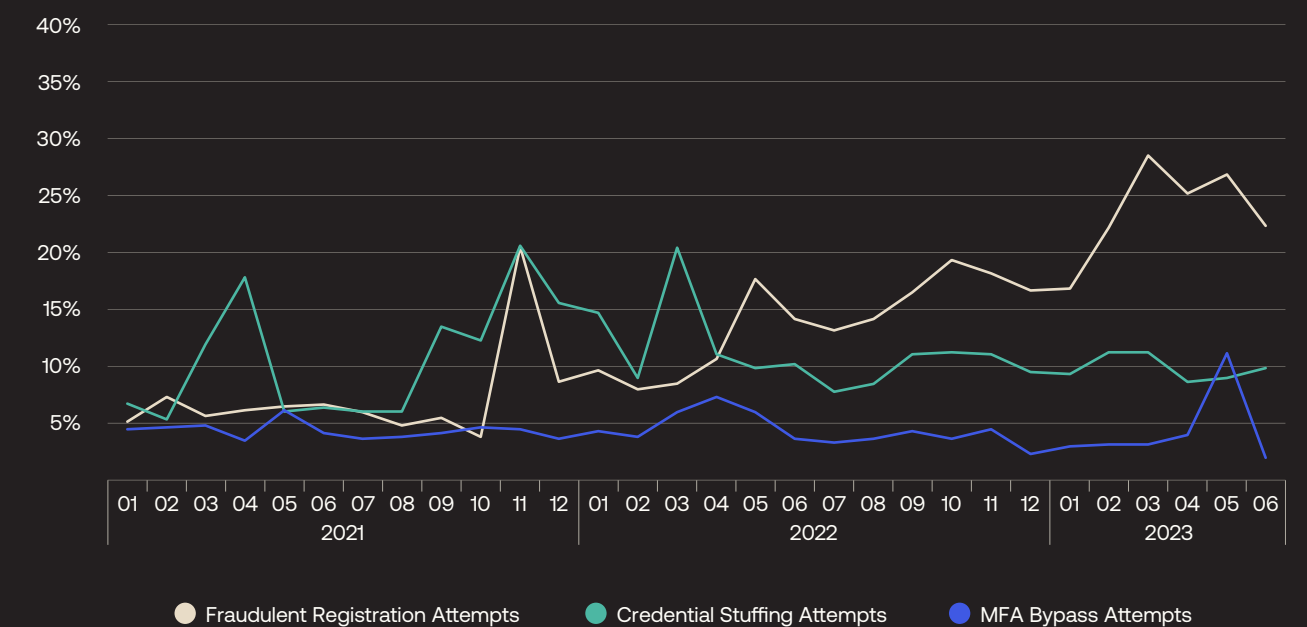


Table 21: United Kingdom

Countries potentially included: England, Northern Ireland, Scotland, and Wales.

Summary of Identity threat trends against organizations headquartered in the United Kingdom

	2021	2022	1H2023
Fraudulent Registration Attempts	5.1%	11.1%	13.6%
Credential Stuffing Attempts	14.5%	12.9%	13.3%
MFA Bypass Attempts	1.6%	2.7%	4.6%

Figure 37: 30-month daily view of Identity threats against organizations headquartered in the United Kingdom

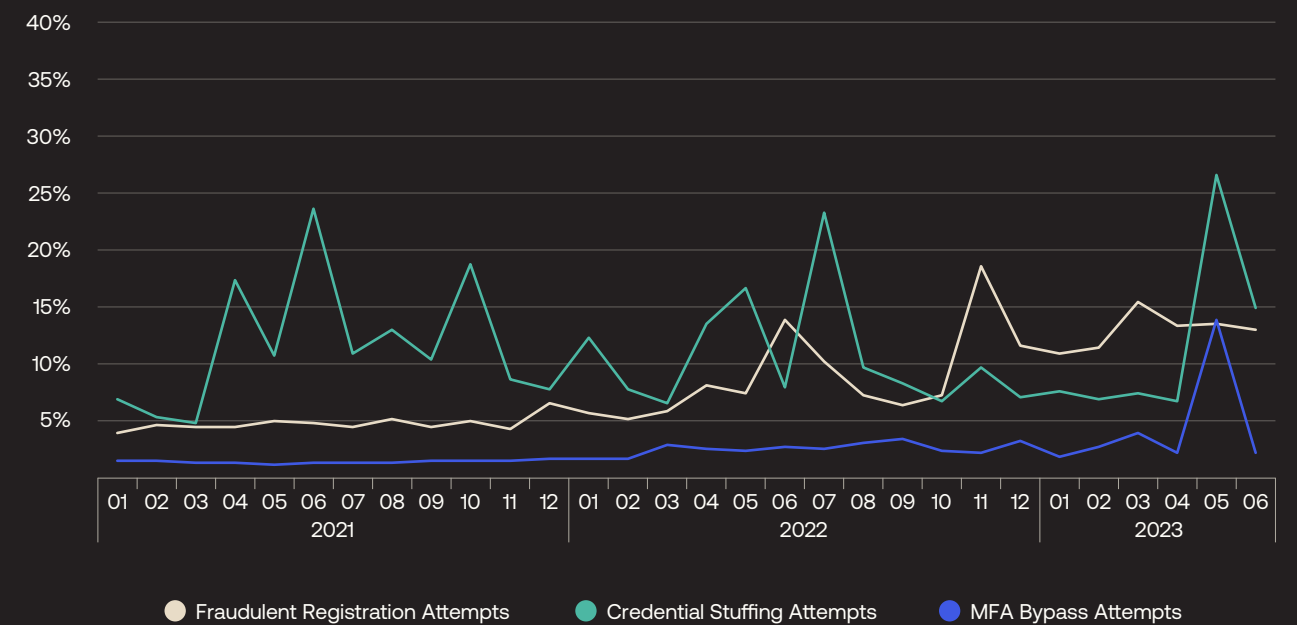


Table 22: Western Europe

Countries potentially included: Austria, Belgium, France, Germany, Liechtenstein, Luxembourg, Monaco, Netherlands, and Switzerland.

Summary of Identity threat trends against organizations headquartered in Western Europe

	2021	2022	1H2023
Fraudulent Registration Attempts	14.6%	28.7%	5.1%
Credential Stuffing Attempts	22.7%	11.2%	6.3%
MFA Bypass Attempts	10.8%	11.1%	14.5%

Figure 38: 30-month daily view of Identity threats against organizations headquartered in Western Europe

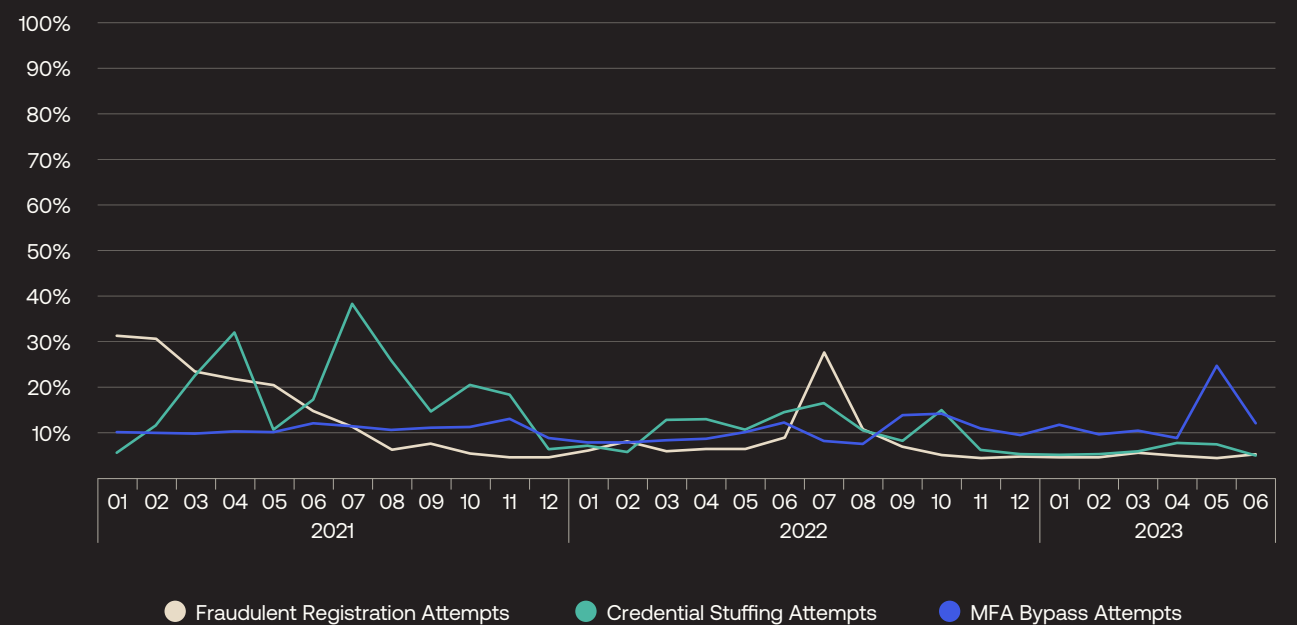


Table 23: Asia-Pacific

Potentially includes any countries within the United States Federal Aviation Authority's [listing of countries in Asia-Pacific](#).

Summary of Identity threat trends against organizations headquartered in Asia-Pacific

	2021	2022	1H2023
Fraudulent Registration Attempts	52.4%	28.9%	27.9%
Credential Stuffing Attempts	55.0%	24.3%	13.3%
MFA Bypass Attempts	6.9%	10.3%	11.0%

Table 24: Japan

Summary of Identity threat trends against organizations headquartered in Japan

	2021	2022	1H2023
Fraudulent Registration Attempts	16.5%	33.9%	43.6%
Credential Stuffing Attempts	4.1%	2.7%	2.4%
MFA Bypass Attempts	25.3%	16.6%	21.2%

Figure 39: 30-month daily view of Identity threats against organizations headquartered in Asia-Pacific

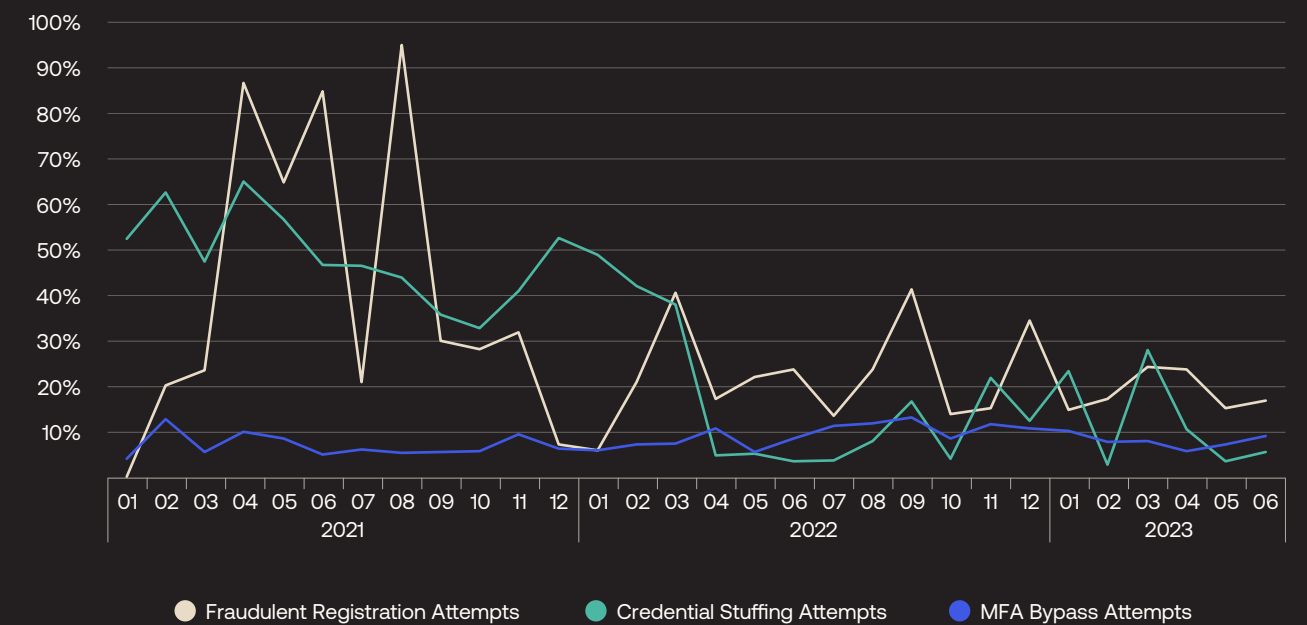


Figure 40: 30-month daily view of Identity threats against organizations headquartered in Japan

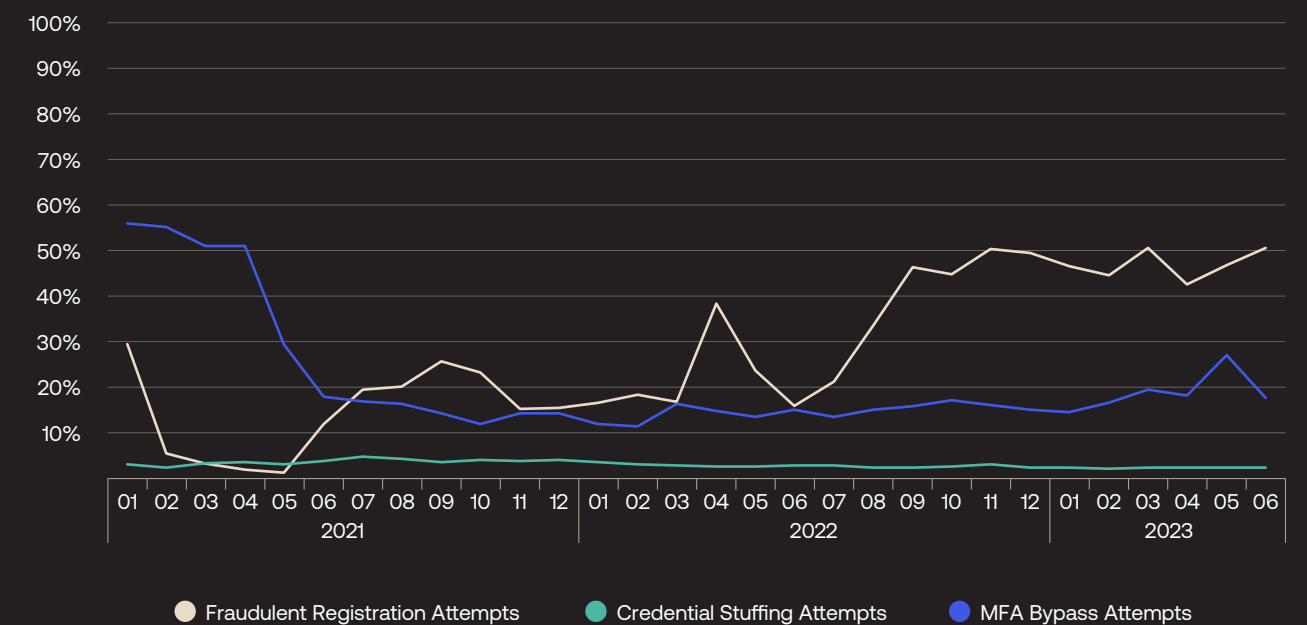


Table 25: Australia & New Zealand

Summary of Identity threat trends against organizations headquartered in Australia or New Zealand

	2021	2022	1H2023
Fraudulent Registration Attempts	53.0%	29.1%	26.7%
Credential Stuffing Attempts	57.1%	26.6%	14.8%
MFA Bypass Attempts	4.3%	8.7%	9.1%

Table 26: Southeast Asia

Countries potentially included: Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

Summary of Identity threat trends against organizations headquartered in Southeast Asia

	2021	2022	1H2023
Fraudulent Registration Attempts	47.3%	15.2%	16.2%
Credential Stuffing Attempts	73.4%	55.8%	24.3%
MFA Bypass Attempts	16.2%	34.7%	3.5%

Figure 41: 30-month daily view of Identity threats against organizations headquartered in Australia or New Zealand

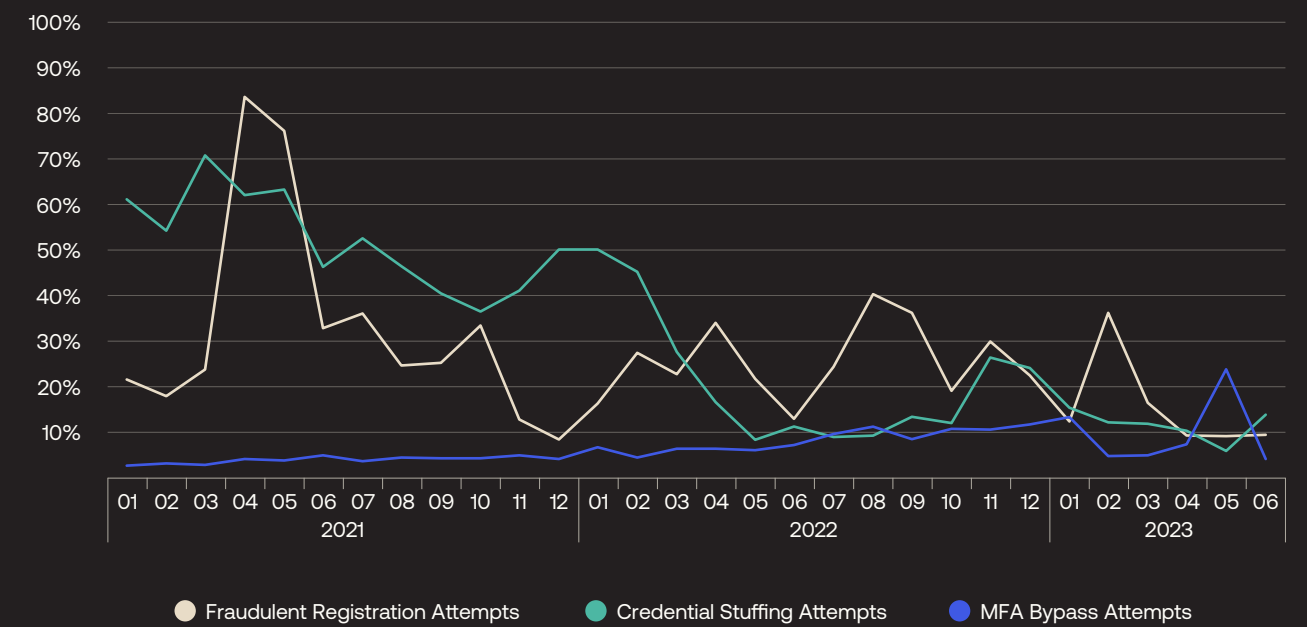
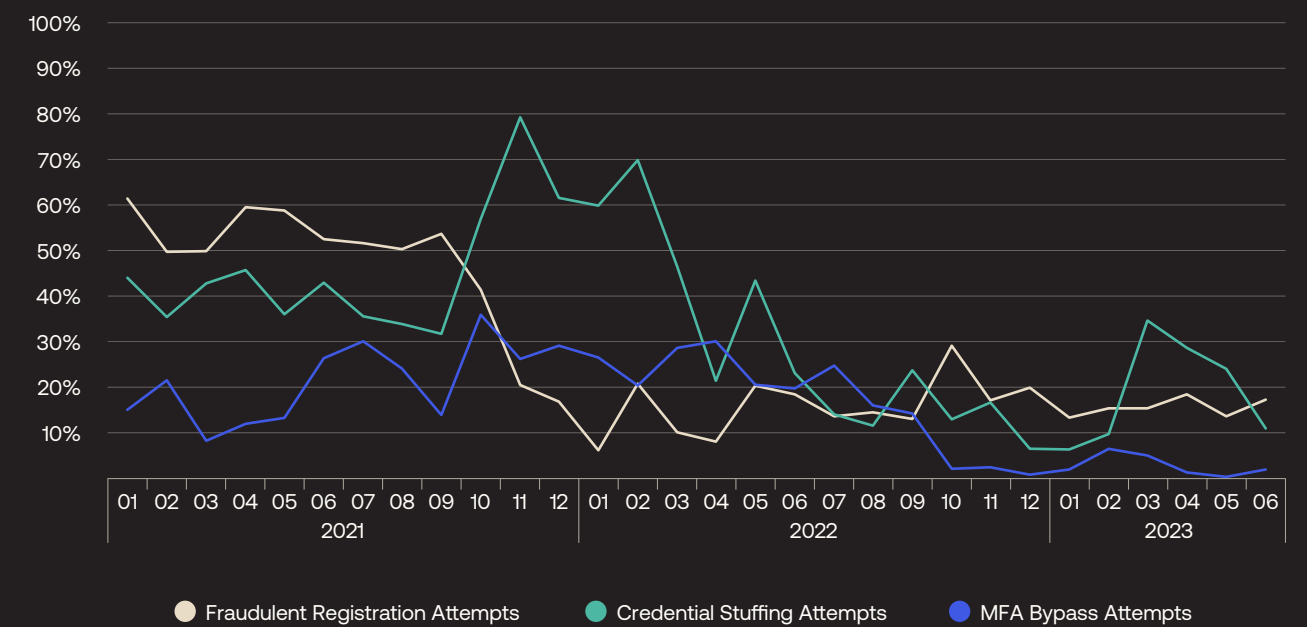


Figure 42: 30-month daily view of Identity threats against organizations headquartered in Southeast Asia





okta

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