Fingerprint

Guide to understanding & preventing account takeover fraud

KEY TRENDS AND STATISTICS

Table of contents

Introduction to account takeover fraud

Account takeover (ATO) attacks are one of the most common and most devastating types of fraud for both consumers and businesses — and it's on the rise.

According to IBM's "Cost of a Data Breach Report 2024", the average cost to businesses is $4.62 million for one data breach involving stolen credentials due to operational downtime, lost customers, and mitigation costs.

The average cost of one data breach involving stolen credentials is

$4.62 million

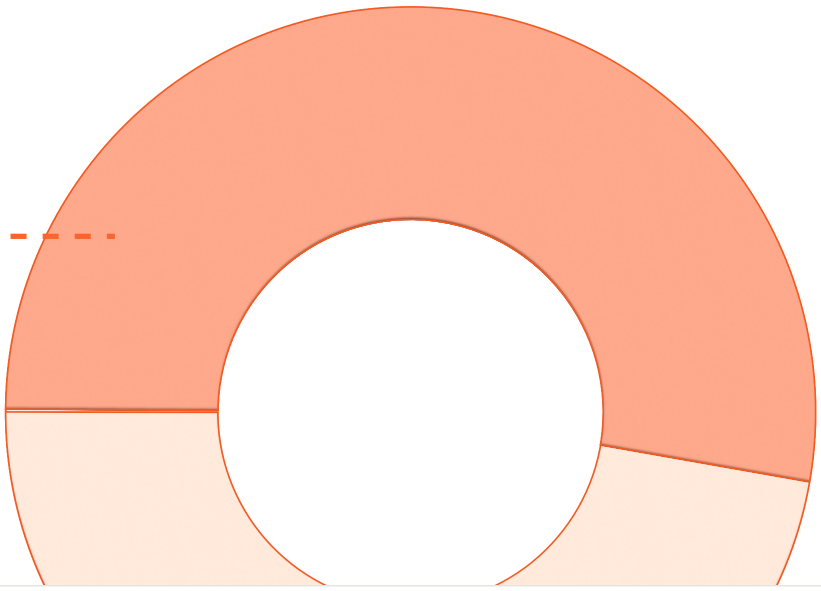
On top of that, the Identity Theft Resource Center reported that account takeover fraud was the most reported form of "identity misuse" in 2023 at 52%. That's not surprising, considering that 29% of U.S. adults surveyed shared that they were victims of ATO fraud in 2023, compared to 22% in 2021. Additionally, with new technologies like generative AI at their disposal, fraudsters are getting better at stealing credentials and gaining unauthorized access to user accounts to steal valuable personal identifiable information (PII), credit card numbers, and more.

Based on those numbers, it's clear that businesses could greatly benefit from the ability to quickly detect and prevent account takeover attacks in order to preserve customer trust and loyalty, and prevent financial losses.

This guide dives into the top trends in account takeover fraud, the impact it has on consumers and businesses, common attack vectors, and what steps companies can take to detect and prevent ATO fraud.

52%

reported that account takeover fraud was the **most reported form of "identity misuse"** in 2023



Trends in account takeover fraud: Generative AI and bots

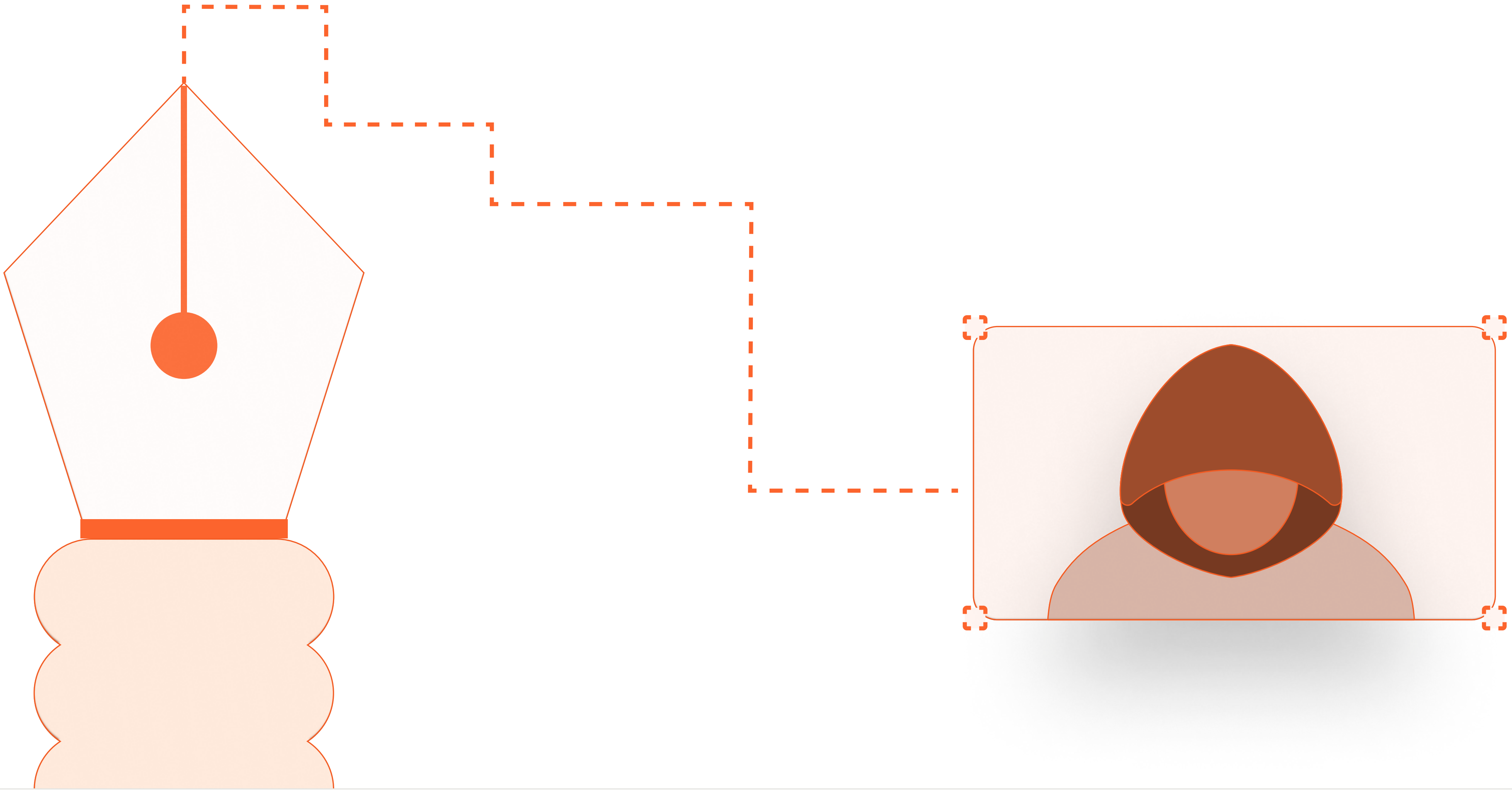
The fraud landscape is always changing because fraudsters adopt new technologies and become more creative with their attacks. For instance, some are contacting job applicants with fake job offers to collect personal identifiable information (PII) like Social Security numbers and dates of birth, which can be used to bypass some verification processes to gain unauthorized access to accounts or even create new accounts.

Others are using generative AI (Gen AI) to create more convincing messages to use in spear phishing emails and SMS messages. For example, a fraudster may use the Gen AI content to send a text that sounds like it's coming from a bank, asking the customer to confirm a deposit or some other action and providing a link to log into the bank's website.

Believing the text to be legitimate, the customer clicks on the link, which takes them to a fake site that looks just like the bank's real login page. The customer then provides their login credentials, unwittingly giving the fraudster full access to their bank accounts to order new debit cards, apply for credit cards, change phone numbers and addresses, and more.

Fraudsters are also using Gen AI to program bots to perform specific tasks online. These can include legitimate tasks like indexing web content for search engines, but they can also launch cyber attacks or perform unauthorized web scraping to gather information for spamming, phishing, or other fraudulent activities.

In the context of ATO attacks, fraudsters typically use automated bots to test stolen username and password combinations across various websites and applications, which we'll cover more in the next section.



Common ATO attack vectors

There are many ways a fraudster can execute an ATO attack, and each one exploits different weaknesses. We'll cover some of the most common ones in this section.

Credential stuffing

Credential stuffing is one main reason why security experts recommend that users do NOT use the same login credentials across different websites. In this type of attack, fraudsters take stolen login details from one data breach and try it on multiple other sites because they're betting on people using the same username and password across multiple services. This tendency to reuse login credentials is a key vulnerability that increases the chances of users becoming victims of an ATO.

Phishing

In phishing attacks, fraudsters pretend to be legitimate companies or people their victims may know in order to trick unsuspecting users into sharing sensitive information like usernames, passwords, or credit card details. They usually try to phish for information through emails and texts — and as mentioned earlier, many fraudsters are now using Gen AI to craft more effective phishing messages to trick their victims.

Brute-force attacks

Brute-force attacks happen when fraudsters use automated programs (aka bots) to quickly try numerous passwords in a short period of time, with the hopes of finding the right one. This approach can be especially effective against accounts with weak passwords or reused passwords, and against businesses that don't use security measures like lockout policies or multi-factor authentication (MFA).

Social engineering

Social engineering happens when bad actors use psychological tricks to make people break security rules. This approach requires little to no technical skills; instead, what's key is the ability to manipulate people by posing as authority figures or trusted colleagues, creating fake scenarios that provoke urgency or fear so that victims are compelled to act quickly without taking extra steps to verify facts. (E.g., if you've ever received an urgent, overly formal text message from your CEO asking you to buy several $100 Amazon gift cards, then you've been targeted in an attempted social engineering scam.)

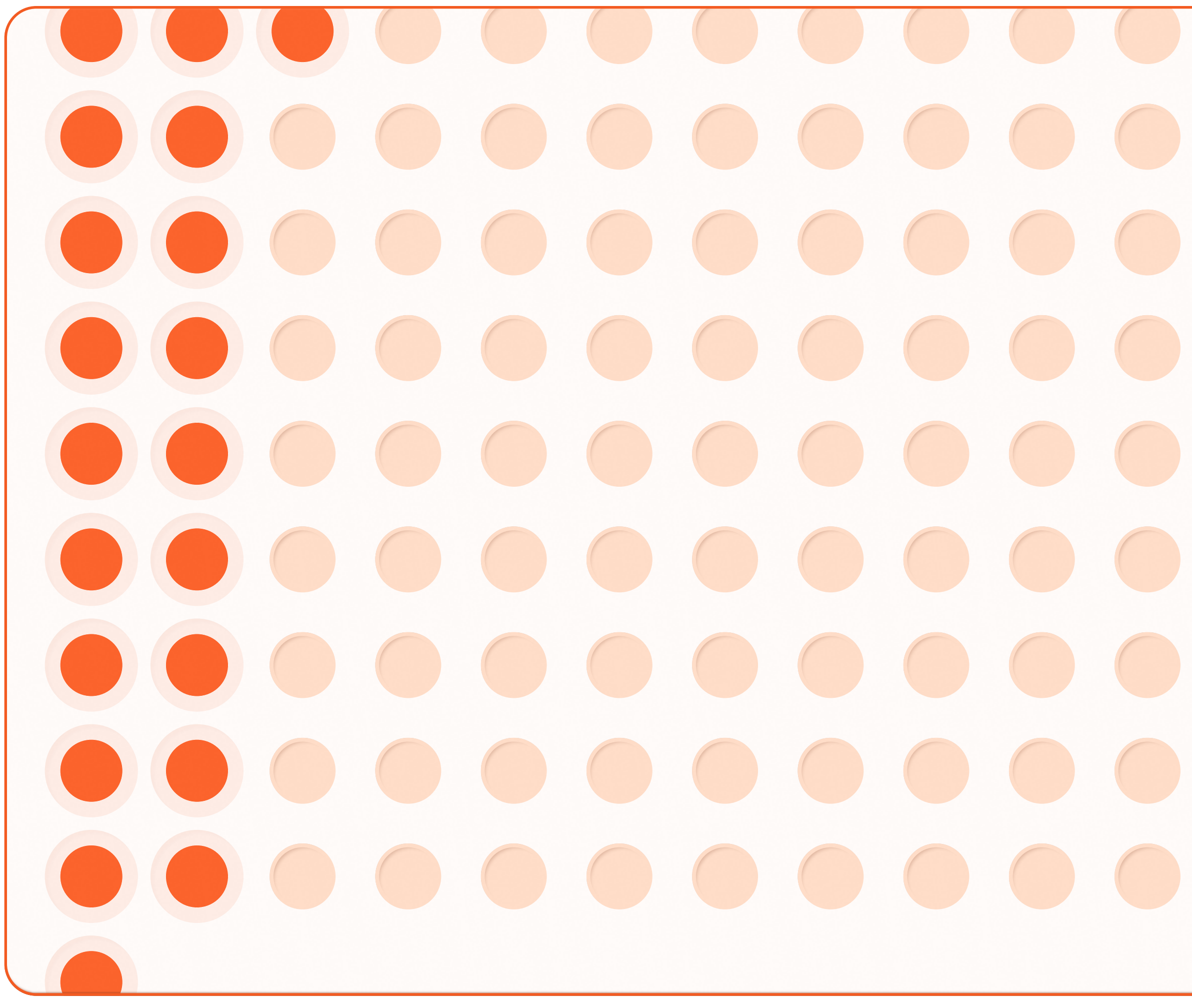
ATO attacks continue to increase — latest statistics and financial impact

ATO attacks have steadily increased over the years, causing significant financial losses for both consumers and businesses. According to one study, ATO fraud was the cause of nearly $13 billion in losses for consumers and businesses in 2023. For businesses, the average cost of just one data breach involving stolen credentials in 2024 is calculated to be $4.62 million due to operational downtime, lost customers, and mitigation costs.

Abnormal Security's "2024 State of Cloud Account Takeover Attacks" shares the results from their survey of over 300 security professionals globally and found that respondents were the most concerned about ATO attacks than any other type of fraud (67.4%).

83%
of security professionals reported that their organization was hit by an ATO attack at least once in the past year

45.5%
of companies were impacted by ATO attacks more than five times over the past year



Nearly **20%**
of survey respondents said their organization experienced **more than 10 significant ATO attacks** in 2023.

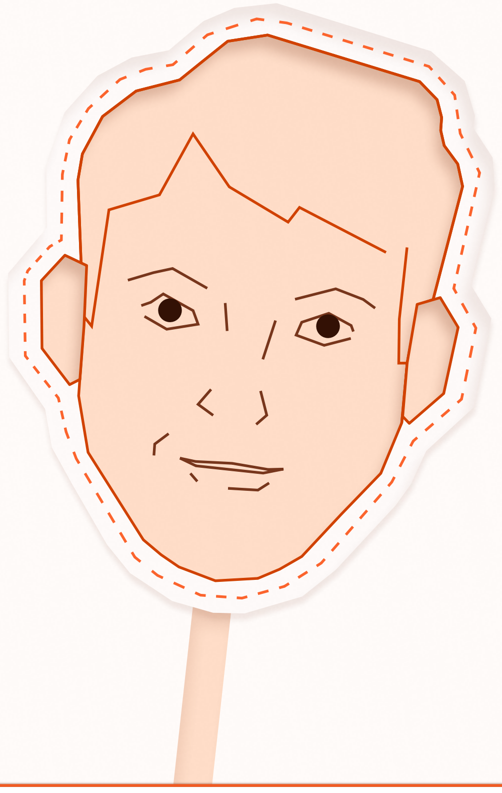
But it's not just businesses who are suffering losses. Consumers are feeling the pain of ATO attacks as well. In its "2023 Trends in Identity Report," the Identity Theft Resource Center shared that account takeovers were the most reported form of identity misuse, with 52% of survey respondents sharing that they were victims of an ATO. In a separate study, 29% of U.S. adults shared that they were victims in 2023.

Impact of account takeover fraud on consumers and businesses

For consumers, dealing with an account takeover is stressful and can be time-consuming. It could be days or weeks before a victim gets refunded for unauthorized purchases or regains access to a compromised account.

40%

of ATO victims also experience identity theft



To make it worse, 40% of ATO victims also experience identity theft, which can negatively impact their credit scores and lead to further financial issues in the future.

But repercussions of ATOs extend beyond just the individual victims — resentment can build towards the businesses that failed to protect them from these potentially devastating attacks. And companies, regardless of industry, will need to deal with the negative fallout of ATO fraud in the form of financial losses, broken customer trust, reputational damage, and possible regulatory action.

For example, one of the largest hotel chains, Marriott, experienced a data breach that went undetected from 2014-2018. A fraudster had taken control of an administrator account to make a database query. As a result, up to 500 million guests had their personal details, passport numbers, and payment information stolen.The attack led to multiple class-action lawsuits and a hefty $23.8 million GDPR fine.

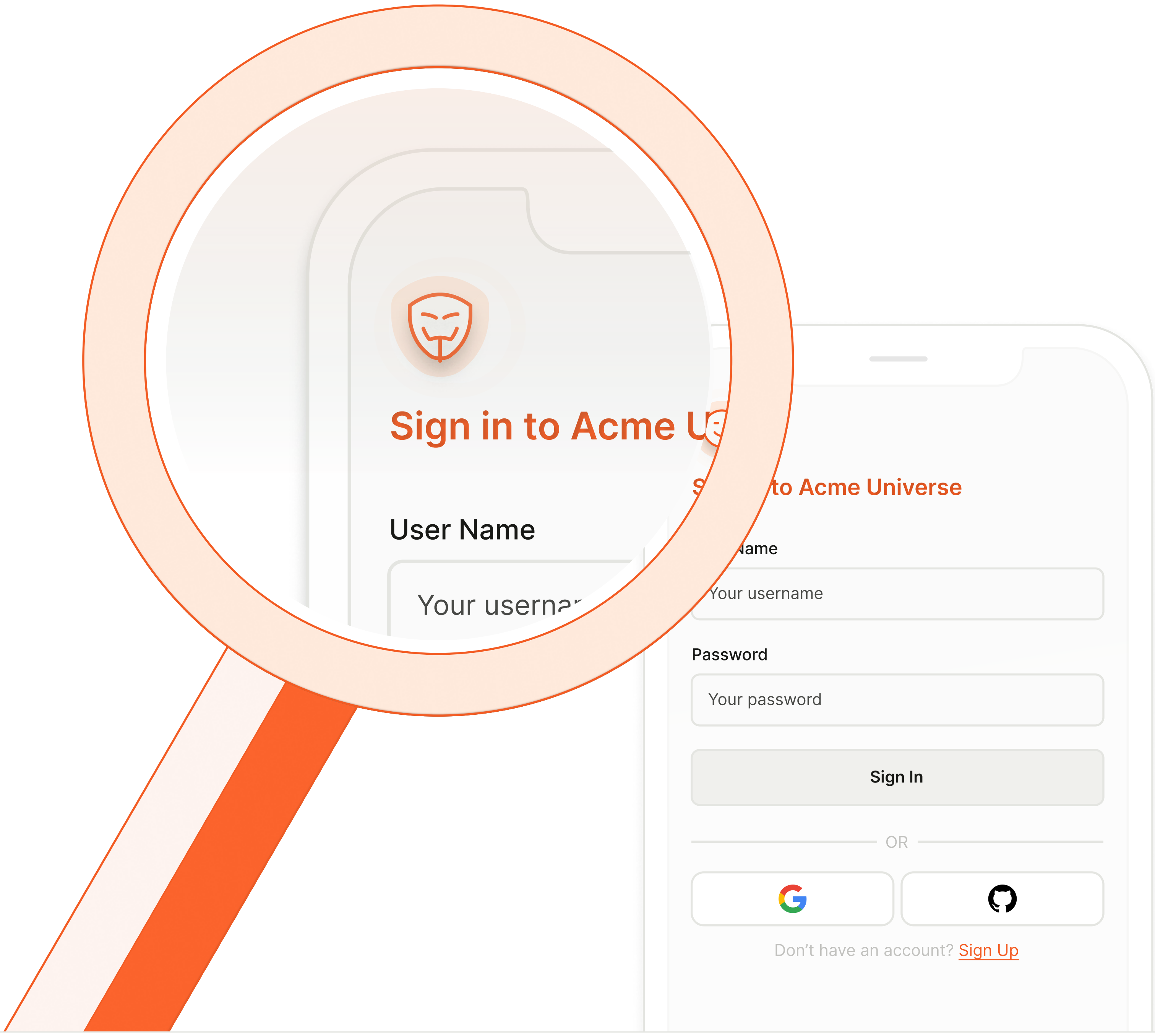
More recently, data giant Snowflake made the news when the company shared that data from ~400 organizations had been compromised. Snowflake is now currently subject to a class-action lawsuit and a Senate investigation. Customers affected include well-known names like AT&T, Santander Bank, and Ticketmaster.

Impact of account takeover fraud on user experience

As we mentioned, consumers who have been victims of an ATO attack typically will lose trust in businesses that failed to protect them, their data, and their money. In attempts to stave off reputation-damaging and potentially financially devastating ATO attacks, more companies are requiring extra authentication steps for users, including multi-factor authentication (MFA), two-factor authentication (2FA), and one-time passwords (OTP).

There are downsides of implementing these extra security steps, however, including higher overall costs and friction for legitimate users. Customers want protection from fraud, but they also don't want to be overprotected — for example, 22% of online shoppers say they abandoned their carts due to too long or too complicated checkout processes.

Plus, while these methods are considered a "gold standard" in ATO prevention in the cybersecurity industry, Abnormal Security reported that only 37% of survey respondents said they're confident these authentication methods can effectively prevent ATO attacks. So what can businesses do to shore up their fraud prevention efforts without degrading the user experience for their customers?



How businesses can protect against account takeover fraud while providing a seamless user experience

Effectively preventing account takeover fraud without frustrating legitimate users can be tricky. Below are some recommendations businesses can take.

Implement strong password policies

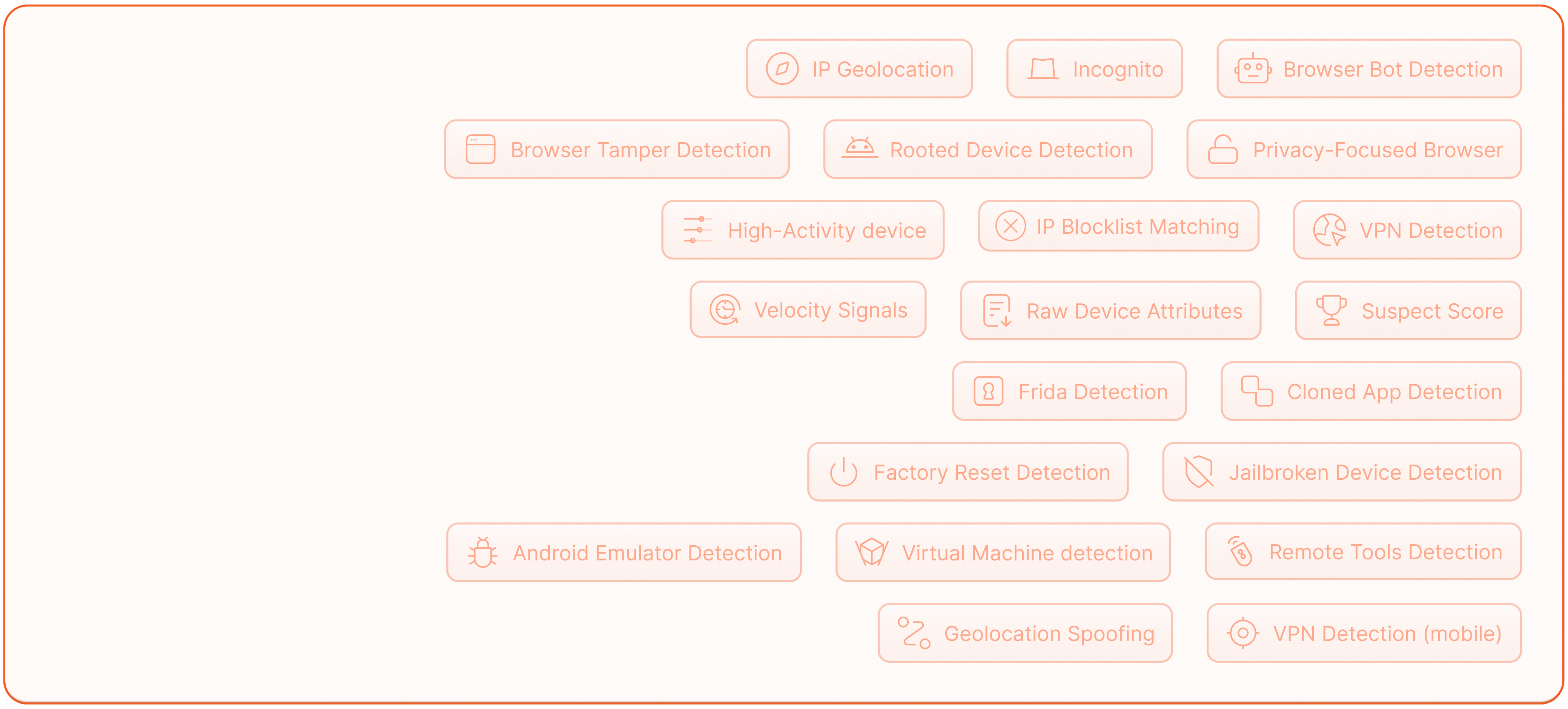
Enforce robust password policies for customers and employees. Requiring complex passwords that combine numbers, letters, and symbols can help significantly reduce the risk of successful account takeover attempts simply because it makes it harder for attackers to guess or crack passwords.

Set rate limits on login attempts

Want to reduce the effectiveness of brute-force attacks? Set policies to lock accounts for a period of time after several failed login attempts while also sending an email or text message to the account holder.

Use an account takeover solution

Specialized ATO solutions that use machine learning and behavior analysis can accurately detect unauthorized access attempts by analyzing patterns and deviations from normal user behavior, like logins from new locations, in real time. For example, a device intelligence solution like Fingerprint collects 100+ signals across devices and browsers to identify all online visitors with industry-leading accuracy, enabling businesses to respond to potential threats in real time.



How Fingerprint can help prevent ATO fraud

Fingerprint is designed to prevent fraud by analyzing device and browser attributes to generate unique visitor identifiers. Fingerprint's proprietary Smart Signals collect user behavior, network, and device signals like VPN usage, browser tampering, and bot activity to help businesses detect suspicious activity and make real-time, data-driven decisions.

For example, when a user attempts to log into a website, businesses can compare Fingerprint's visitor ID to determine whether the login is coming in from an unknown device or from an unfamiliar location.

If the answer is yes, then the user will be requested to provide an additional form of authentication, like a one-time password (OTP). However, since Fingerprint also recognizes legitimate user visitor IDs, this extra step only needs to be activated for unknown users or when suspicious activity is detected.

ATO DETECTION AND PREVENTION

Key takeaways

Account takeover fraud is a prevalent and increasing threat that continues to evolve as fraudsters become more sophisticated and creative in their methods. As we've outlined in this guide, the impact of ATO attacks extends beyond financial losses.

To preserve customer loyalty, protect brand reputation, and prevent potentially significant financial losses, organizations need to be proactive when it comes to guarding against ATO fraud. Using traditional authentication methods like MFA or OTP alongside newer technology like Fingerprint's device intelligence platform enable companies to better protect customer and company data while delivering seamless user experiences.

Want to learn more about how Fingerprint can help you detect and prevent ATO fraud? Contact us today for a personalized demo — or if you prefer exploring yourself, sign up for a 14-day free trial.