How to detect early signs of Customer Acount Takeover and Bad Actor Accounts.

By Beery Holstein, Senior Product Manager

Hackers are getting far more creative with account takeovers (ATO) and bad actor account creation. We're seeing them invade established customer accounts at many points in the identity lifecycle — not just at login. And when bad actors register new accounts, they are typically laying the groundwork for attacks downstream.

Sure, you can add multi-factor authentication (MFA) and continue using your transaction-focused fraud tools. But that's still not enough. Plus, piling more friction in the customer's path is bad for business.

The reality is: attackers can slip into customer accounts or make malicious moves *after* the login. Waiting to catch them while they're making a purchase or moving money out of a customer's account is too late. If they breach private customer information or sensitive data, it damages your brand. Customers who lose trust will take their business elsewhere.

Consider this analogy. Would you use two locks on the front door of your house and a third lock on the safe where you keep your jewels, only to let a burglar crawl in a window, wander around your home and riffle through papers on your desk? In the ATO scenario, bad guys compromise data and security — even if they don't transact.

In this article, I'll explain how to stop ATO and bad actor accounts in real time, before a security breach. Early detection is critical, and I'll explain how to do it in a way that will also improve the customer experience (CX).

Account abuse is skyrocketing

Without the right security in place, financial institutions, etailers, service providers and app owners all feel the strain. A 2021 Juniper Research report shows US companies lost $25.6B to ATO fraud in a single year. And it's not just theft of monetary assets but personal information. Any security breach can shake customer trust and hurt revenue.

Motivated by money

What's fueling the rise in ATO? Cybercriminals work together in an ecosystem of fraud. It's a well-orchestrated business on the dark web with many people probing for vulnerabilities, testing new attack vectors and sharing tricks. It's the same underground where hackers sell stolen credentials and toolkits that make it easy to strike fast, at scale. Some bad actors have the patience to go 'low and slow' in an attempt to look like a legitimate customer. Either way, they often leave a trail...

Signs of ATO fraud or bad actor accounts

One red flag is rarely enough. Most signs of ATO or bad actor account fraud come to light in complex combinations. It's like solving a Rubik's Cube, a simple 3-inch block. How hard can it be? Well, a Rubik's Cube has 43-quintillion combinations but can be solved in 20 moves. Point being, ATO detection is difficult but can be done — long before you're hit with chargebacks or support calls from upset customers.

Security must be intelligent and contextual to examine hundreds of signals, correlate that data with up-to-the-minute threat intelligence and compare it to the customer's typical behavior. To avoid disrupting your good patrons, real-time risk assessments must be highly accurate. Too many false positives will only add friction and annoy customers. So try not to overreact to one bad signal, and keep in mind, this list is the tip of the iceberg:

1. Aberrant behavior

By knowing your unique customer and monitoring that specific individual's account activity and login patterns, we can detect anomalies that may indicate an ATO. It warrants deeper inspection, for example, if a user:

- Logs in from a new device
- Uses a different browser than is typical
- Connects from different locations or time zones; impossible travel
- Uses a new cellular service (ASN)
- Strays from "normal" behavioral biometrics, like mousing dynamics
- Changes account details, such as a new password, email, phone number

Threat behavior is always changing, so this is not a complete or static list. It's also worth repeating: one change is rarely a sign of fraud. It's crucial to have advanced security with the intelligence to identify combinations of high-risk signals.

As you continually look for risk, you are also building a complete profile of your customer. When you know it's your customer with a high level of confidence, you can remove friction by extending the user session or reducing the need for MFA. Stronger security improves the CX. There's no need to compromise.

2. Password resets and account changes

Password resets — especially in the call center — can be a red flag if you see other risk signals along with it. Weaknesses in the account recovery process and call center verification make it one of the easiest, most popular ways to take over customer accounts.

When a hacker takes over an account, they may try to change account details, like the email address or phone number. They do this so they can recover and maintain control of the account while locking out the real customer. In the process, hackers also look for personal information that can help them pull off other scams, like opening credit in the customer's name. These are big pain points that can be prevented.

3. Suspicious IP addresses

A new IP address or geolocation could indicate your customer is traveling... or it could be suspicious since IP address changes can indicate a fraudster is trying to intercept communications. For example, a spoofed IP address may be used in a man-in-the-middle attack to conceal the attacker's own identity. If the geolocation matches the customer's usual location, but the device is hidden behind a proxy, consider this a risk factor.

4. Multiple accounts, same device

Unless a fraudster masks their device data, you may see a user log into multiple accounts with the same desktop or mobile. You'll want to keep an eye on this one, but don't act too quickly because family members often share the same device. You'll need strong device fingerprinting to collect information about a customer's trusted devices (type, model, CPUs, screen size, etc.) throughout the digital journey. An atypical device or swapping between devices mid-session could indicate session hijacking or device compromise.

5. Device spoofing

Much like a spoofed IP address, fraudsters use device spoofing to cloak their identity. By masking their device data, device details either appear as "unknown" or don't match the real customer's device data. There is a high risk of fraud if you see a pattern of accounts that are connected to more "unknown" devices than legitimate ones. You should be able to see the exact device details, and those details should remain consistent.

6. Device emulators

Imagine device spoofing on steroids. Using device emulators, fraudsters can not only spoof a device's make and model ID, but they can go into advanced settings to change the OS version, CPU processor and more. Most alarming, they can emulate thousands of mobile devices at the same time.

These robust capabilities enable attackers to repeat many login attempts without getting locked out of an account. Instead, every attempt appears to be a user trying to log in from a different device each time. Detecting a device emulator is a strong indicator of fraud since its only legitimate use is to run an app in a test environment.

7. Bot behavior

When cybercriminals use credential stuffing to break into customer accounts, they typically enlist bots to automate the process of testing logins across thousands, if not millions of accounts — very quickly. To detect these bot-powered attacks, you need the ability to detect bot behavior, such as:

- Automation frameworks
- Velocity rates
- Bot-like text input or mouse movements

This is far from an exhaustive list and like all threats, bot behavior evolves. It's also worth noting that many companies rely on CAPTCHA to prevent bots from logging in and taking over customer accounts, but low-cost tools, like Anti-CAPTCHA, are now widely available and make it easy for hackers to bypass this once-dependable security measure.

> *Digital identity fraud continues to rise. Account takeover (ATO) jumped 90% and bad actor account creation increased 109%, reveals Javelin Research.*

Account protection = Business enabler

Protecting customer accounts with modern customer identity and access management (CIAM) services is a business enabler. When done right, stronger security creates better customer experiences. It should also be easier to manage, so you can improve effectiveness and efficiency while lowering costs. To do all of this, you must be able to:

1. **Stop account abuse much sooner** – We've covered this above. It's complex and sophisticated, not a single point in time but any point in time. Continuous real-time risk and trust assessments are essential.

2. **Reduce friction** – Know your trusted customer and how they behave so you can cut back on friction. Stronger security and better experiences are no longer a tradeoff. You can have both by building a profile of your trusted customer and weighing that against known risk behaviors and up-to-the-minute threat intelligence. It's a rare case when stronger security creates better CX.

3. **Gain visibility** – You can't mitigate risk in the absence of data or in a silo. Security teams and fraud teams must be able to measure risk, see trends and have the data to make the right cyber identity decisions. Without it, how can you explain to executives or customers when access is denied?

4. **Simplify** – Integrating and aggregating multiple vendor solutions or home-grown CIAM can be overwhelming. Complexity costs you in terms of maintenance, CX and keeping your security posture in the face of evolving threats. Even with a single vendor, you want it to be a no-brainer so your developers say, "Yes, this is easy. We can do this quickly, in a short sprint." The right solution will speed time to value so you immediately mitigate risk, elevate trust, improve CX and boost visibility.

How Transmit Security mitigates ATO fraud

By now, you get the scope of the problem. Key takeaway: it requires a dynamic risk and trust engine to assess hundreds of signals in real time. You need contextual, intelligent security powered by machine learning (ML) continuously trained on the latest attack methods. It's mission-critical to keep pace with the market and threat dynamics.

Advanced Security and Verification Services automate a rapid response to signs of ATO fraud and bad actor accounts throughout the identity lifecycle. Our cloud-native services are modular so you can roll out the solutions you need most and expand later.

- **Advanced Security Services** continuously detect and mitigate risk to stop account abuse the instant signs appear. Our solution simultaneously builds trusted customer profiles to identify good users and minimize their friction. When risk is detected in real-time, you can elevate trust by authenticating the user with our Passwordless and MFA Services or proving their ID with Identity Verification.
- **Identity Verification Services** prevent bad actor account creation before enrollment or anytime it's needed. Native document verification, ID proofing and liveness checks make it highly accurate, easy to use and more cost effective.

Developer-friendly APIs make it quick and easy to turn identity security into a business enabler. You can immediately: 1) stop account abuse; 2) reduce friction and 3) gain visibility.