ACCOUNT TAKEOVER PREVENTION

COMPLETE GUIDE

How To Detect and Prevent ATO Fraud Attacks

spec

Increasing ATO Attacks

Account takeover fraud is increasing due to stolen credentials, phishing, malware, and bots, leading to data theft and financial damage. This results in lost revenue, reputational harm, and decreased customer trust. With rising data breaches, ATOs are projected to surge in 2025.

$13b

Global estimated ATO fraud losses

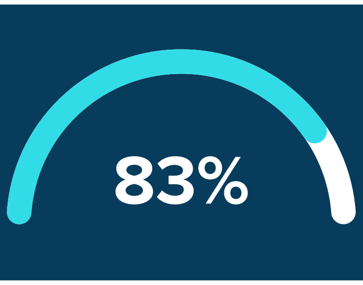
This guide dives into ATO fraud, how it works, and why proactive prevention is critical. Learn about practical steps and cutting-edge tools like Spec Customer Journey Security to secure your business.

What Is Account Takeover Fraud?

Account takeover fraud occurs when a cybercriminal gains access to an online account using stolen credentials, allowing them to steal funds, make unauthorized purchases, or commit further fraud. Unlike general identity theft, ATO specifically targets accounts like banking, eCommerce, or loyalty programs, compromising the victim’s digital identity and access.

What Are Real-World Examples of ATOs?

Notable account takeover fraud incidents include the Marriott data breach from 2014 to 2018, where attackers accessed the personal and financial data of 500 million guests, leading to lawsuits and a $23.8 million fine. In 2018, the Ticketmaster hack exposed thousands of customers’ payment information and personal details using malicious software.



Organizations that experienced at least one ATO in the past year

Common ATO Techniques

Account takeover attacks often start with fraudsters collecting credentials or personal data. Once inside an account, they secure control and conceal their activity.

Phishing

Fraud emails or messages trick victims into clicking malicious links or entering login credentials on fake websites.

Smishing

SMS-based phishing asks victims to click malicious links or share sensitive data, often with account issue claims.

Vishing

Fraudsters use voice calls to manipulate victims into disclosing passwords or private information.

Credential Stuffing

Attackers use stolen credentials from data breaches to try logging into other accounts, hoping for passwords reuse.

Brute Force Attacks

Automated tools systematically guess passwords, often targeting accounts with weak or default credentials.

Social Engineering

Attackers exploit victims by building trust or creating fear to extract sensitive info or circumvent security.

Malware

Malicious software records keystrokes, screenshots, or browsing activity to steal passwords or other data.

Data Breaches

Attackers exploit compromised databases containing millions of stolen credentials to access accounts.

SIM Swapping

Fraudsters convince mobile carriers to transfer a victim's phone number to a new SIM card to intercept 2FA codes.

Man-in-the-Middle

Cybercriminals intercept unencrypted traffic on public Wi-Fi networks to collect sensitive info like login details.

ATO Attack Process

Account takeover attacks all share a common thread: exploiting vulnerabilities to gain unauthorized access. To understand and counter ATO fraud, it’s important to know the steps attackers follow.

1 Gaining Credentials

Attackers use phishing, malware, or data breaches to steal login details. They may also purchase credentials from the dark web or use brute force attacks to guess passwords.

2 Exploiting Security Weakness

Once they have credentials, attackers bypass defenses like weak or absent MFA, outdated software, or unpatched vulnerabilities to gain access.

3 Maintaining Access

After gaining entry, attackers secure their control by changing passwords, updating security questions, and enabling stealth techniques like VPNs or private browsing to hide their activity.

4 Escalating Fraud Activities

Attackers may also escalate their fraudulent activities by adding new payment methods or transferring stolen funds to external accounts they control.

Business Impact of Account Takeover Fraud

ATO fraud isn't just an IT problem, it's a business-critical issue that affects operations, finances, and customer relationships.

When fraudsters gain control of accounts, they don't just exploit the victim. They also harm businesses by eroding customer trust, causing financial losses, reputational damage, and increasing operational costs.

Financial Losses

Account takeovers result in fraudulent transactions, chargebacks, and potential regulatory fines, leaving businesses to cover the financial and legal consequences. In 2023 alone, **ATO fraud led to nearly $13 billion in losses**.

Reputational Damage

Around **73% of consumers believe businesses are responsible for preventing ATO attacks** and securing customer credentials. A single breach can erode trust, drive customers to competitors, and take years to recover from.

Operational Strain

Resolving customer complaints and implementing new safeguards divert resources, increase costs, and slow operations. With **ATO attacks rising 354% last year**, businesses must detect and mitigate fraud effectively.

Why Proactive ATO Fraud Prevention Is Critical

As fraudsters develop more advanced techniques, merchants can no longer rely on reactive measures. By the time an ATO attack is detected, the damage is done.

Proactive prevention provides businesses with the visibility they need to safeguard customer data, reduce losses, and maintain trust.

Stay Ahead of Evolving Threats

Proactive solutions like Spec Customer Journey Security use advanced machine learning to identify risks before they escalate.

Reduce Financial Losses

By preventing account takeover attacks, fraudulent transactions and chargebacks, businesses can protect their bottom line.

Preserve Customer Trust

Demonstrating robust security measures reassures customers, fostering loyalty and confidence in your business.

Streamline Operations

Automated defenses reduce the workload on support and fraud teams, allowing them to focus on other operational priorities.

How to Prevent Account Takeovers

Preventing ATO fraud needs a multi-layered strategy, as cybercriminals exploit vulnerabilities in login processes, session handling, and transaction monitoring.

1 Monitor for Unusual Activity

Real-time monitoring of user behavior is crucial for early detection of account takeover attempts. By identifying patterns that deviate from legitimate activity, you can stop an attack before it escalates.

- Track Behavioral Patterns
- Flag Suspicious Activity
- Monitor Account Changes
- Leverage Spec's 14x Richer Journey Data™

2 Automate Advanced Prevention

Automation allows businesses to stay ahead of attackers by identifying and responding to threats in real-time. Advanced ATO prevention tools use machine learning to detect patterns and adapt to emerging fraud techniques.

- Deploy Real-Time Defenses like Honeypots
- Use Integration Triggers to Automate Protective Actions
- Adopt Tamper-Proof Systems
- Leverage Machine Learning to Analyze Risk

How to Prevent Account Takeovers

3 Employ Device-Level Security

Securing user devices is an essential layer of defense. Attackers frequently exploit unrecognized devices or use tools like SIM swapping to bypass authentication mechanisms. Device-level security adds another checkpoint before granting access to accounts.

- Use Device Fingerprinting
- Implement Behavioral Biometrics
- Monitor Device Anomalies
- Assess Risk Holistically

4 Educate and Train Teams

Even the most advanced systems are only as strong as the people using them. Ensuring that employees and customers understand ATO threats is critical for building a secure environment. By empowering teams and users, businesses can create a stronger, united front against fraud.

- Train Employees Regularly
- Educate Customers
- Share Educational Materials
- Foster Security Awareness

How to Prevent Account Takeovers

5 Protect the Entire Customer Journey

Cybercriminals often exploit points of vulnerability beyond login pages. A truly effective ATO prevention strategy must secure every step of the customer journey, from account creation to transaction completion.

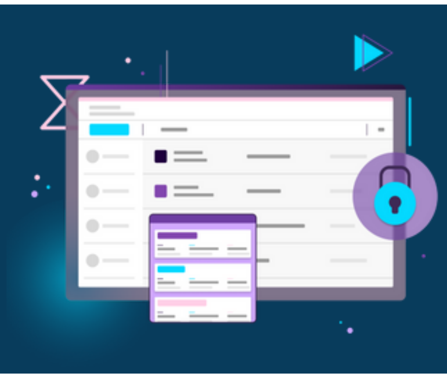
Key Measures for Journey-Level Protection

- Monitor Full User Sessions
- Implement Dynamic Risk Scoring
- Use Cross-Channel Protection
- Enable Journey-Based Blocking

By securing every step of the journey, businesses can stay one step ahead of attackers while providing seamless, uninterrupted service to legitimate users.

Learn how to prevent ATO attacks with Spec!

LEARN MORE



Account Takeover Fraud Prevention: INDIEGOGO

Indiegogo’s Situation

The popular crowdfunding platform needed to reduce account takeovers and prevent losses from fraud-related chargebacks. In only six months with Spec, Indiegogo experienced significant reductions in fraud chargebacks.

337m
Reduction in Attack Pressure

75%
Fewer Fraud Chargebacks

9.8%
Increase in Good Orders

Spec’s Solution

Indiegogo deployed the Spec Customer Journey Security platform, gained end-to-end visibility, and identified the root cause of fraud chargebacks: account takeovers from persistent credential stuffing. Attackers are now funneled into a poisoned honeypot preventing them from transacting and gaining intelligence about Indiegogo’s security and fraud defenses.

> **"Spec makes it simple to understand what’s happening in each of our user flows. When new issues emerge, we’re able to immediately understand what’s really happening and make adjustments instantly."**
>
> - Justin Orme, Payment Lead INDIEGOGO

Stronger Authentication Increases Friction

Some businesses, particularly in banking and high-security industries, implement strict security measures that reduce ATOs but create significant friction for users. For merchants, these defenses can hurt growth and user experience. While they can be effective, they are often not a practical solution for friction-sensitive industries.

🚫 Creating Strong Authentication

Authentication is a strong defense against account takeovers for businesses that are not as sensitive to friction.

- Enforce MFA
- Strengthen Password Policies
- Use Adaptive Authentication

🚫 Limiting Attack Vectors

Attackers exploit vulnerabilities in login systems and networks to infiltrate accounts. Reducing these opportunities is a critical part of a proactive ATO prevention strategy for high-security industries.

- Limit Login Attempts
- Implement CAPTCHAs
- Restrict Suspicious Logins

How To Detect ATO Attacks

Detecting account takeover attempts requires recognizing unusual activity. Early identification of attacks signs can help businesses prevent significant harm.

COMMON ATO ATTACK SIGNALS

Login Attempts from Unusual Locations or IP Addresses

Fraudsters frequently access accounts from regions that differ from a legitimate user's normal activity. Access from unusual IPs, coupled with abnormal browsing behavior, is a strong red flag.

Rapid Changes to Account Details like Passwords or Emails

Fraudsters often modify account credentials to lock out legitimate users. Watch for sudden changes to key information to detect ATO attempts.

Abnormal Behavior in User's Transaction Patterns

Look for transactions that deviate from a user's normal behavior, such as high-value purchases, unusual items, or transactions originating from unexpected locations.

Increased Account Lockouts or User Complaints

A spike in users reporting lockouts may signal an ATO attack. This pattern often coincides with bot-driven brute force or credential-stuffing campaigns.

ADVANCED ATO ATTACK INDICATORS

Login Attempts Linked to Prior Attack Scouting

Fraudsters often test credentials before launching full-scale attacks. Repeated login attempts from the same device or network after suspicious reconnaissance may signal an impending ATO attempt.

Targeted Disabling of JavaScript & Security Features

Attackers disable JavaScript, security scripts, or bot mitigation tools to evade detection. If these features are missing during login, it could indicate an ATO attempt in progress.

Use of VPNs, iCloud Private Relay, or Anonymizing Proxies

Fraudsters mask locations with privacy tools. Frequent logins from anonymized networks, especially combined with other red flags, warrant closer inspection.

Device ID Manipulation & Fingerprinting Evasion

Cybercriminals spoof devices, modify browser settings, or use virtual machines to bypass detection. Monitoring for mismatched device attributes can help flag suspicious activity.

Account Takeover Mitigation

Once suspicious activity is identified, swift and decisive action is essential to protect users and the organization. Implement the following mitigation strategies to disrupt attacks and restore accounts.

Freeze Accounts with Suspicious Activity

Suspend access to compromised accounts to stop fraudsters from executing unauthorized transactions. This can prevent further damage while allowing the legitimate user to regain control.

Authentication for Flagged Behaviors

To combat detected anomalies, prompt users for identity verification using methods like multi-factor authentication (MFA) or security questions to stop fraudsters from proceeding.

Real-Time Alerts to Notify Threats

Automated systems send alerts about suspicious activity to security teams and account owners. Early notifications enable prompt investigation, allowing users to confirm or deny changes.

Monitor Ongoing Account Activity

After addressing an initial incident, continue monitoring the account to detect follow-up attempts. Attackers may return to exploit remaining vulnerabilities or retry compromised credentials.

Restore Account Integrity

Assist users in resetting passwords, reviewing transaction history, and checking for unauthorized changes. Enhance account security with updated security like stronger passwords and additional MFA steps.

ATO Solutions by Industry

Modern businesses face increasingly sophisticated account takeover threats. Traditional security measures are no longer enough to keep fraudsters at bay. **Spec Customer Journey Security** provides businesses with cutting-edge tools to protect accounts proactively while ensuring a seamless experience for legitimate users.

Industry	Vulnerabilities	Spec Benefits
E-commerce and Retail	• Credential Stuffing • Loyalty Fraud • Bot-Driven Attacks • Gest Checkout Exploitation	• Prevents Fraud Transactions • Stops Loyalty Fraud • Blocks Bot Abuse • Secures Guest Checkout
Marketplaces and Ticketing	• Fake Account Creation • Bot-Driven Ticket Purchasing • Promotion Abuse • Transaction Manipulation	• Blocks Fake Accounts • Prevents Bot Hoarding • Protects Promotions • Secures Transactions
Financial Services	• Credential Stuffing and Brute Force Attacks • Unauthorized Fund Transfers • Phishing and Social Engineering • Mobile App Vulnerabilities	• Detects and Blocks Credential Attacks • Monitors High-Risk Actions • Ensures Compliance Security • Protects Mobile Apps

By addressing the unique vulnerabilities of each sector, Spec enables businesses to stay ahead of attackers while providing a seamless and secure experience for legitimate users.

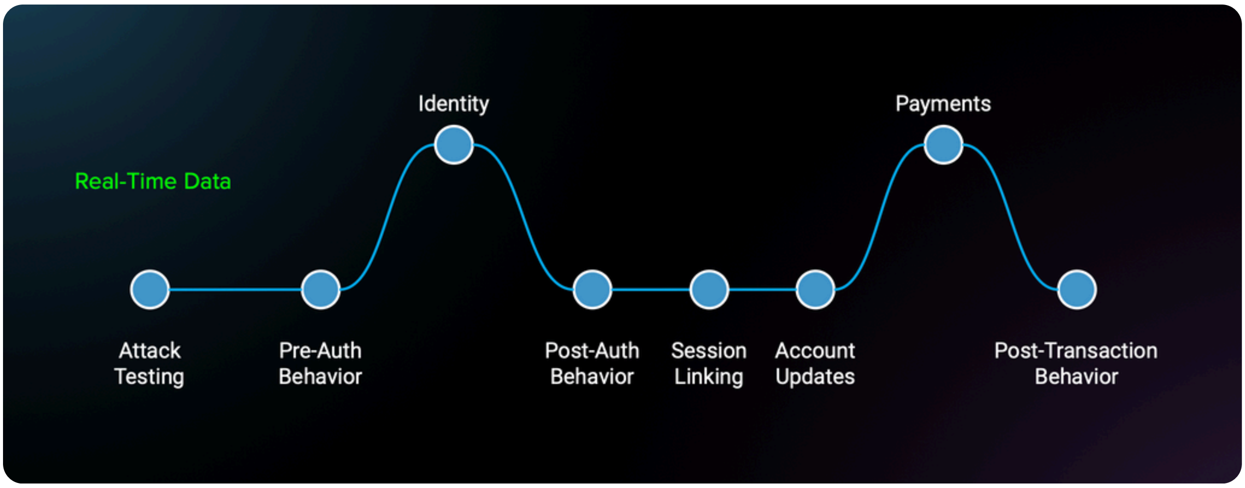
Prevent ATOs With Spec Customer Journey Security

What is Customer Journey Security?

Spec Customer Journey Security goes beyond traditional fraud tools by monitoring and analyzing every user interaction throughout the journey. This comprehensive approach provides deeper insights and allows for more proactive prevention to stop account takeovers before they happen.

How Does It Work?

- ☑ **Journey Data™ Collection:** Captures 14x more data points than traditional fraud systems, offering a detailed view of user behavior at every touchpoint of the customer journey.
- ☑ **Behavioral Modeling and Entity Graphs:** Enables accurate identification of legitimate users versus fraudulent activity modeling behavior across sessions, devices, and IP addresses.
- ☑ **Automated and Invisible Protections:** Uses techniques like honeypots and redirects to block fraud without affecting the experience of legitimate customers.



Why Choose Spec Customer Journey Security?

What Makes Spec Different?

Spec stands out among fraud prevention companies due to our comprehensive approach, advanced technology, and access to 14x more data than traditional fraud systems.

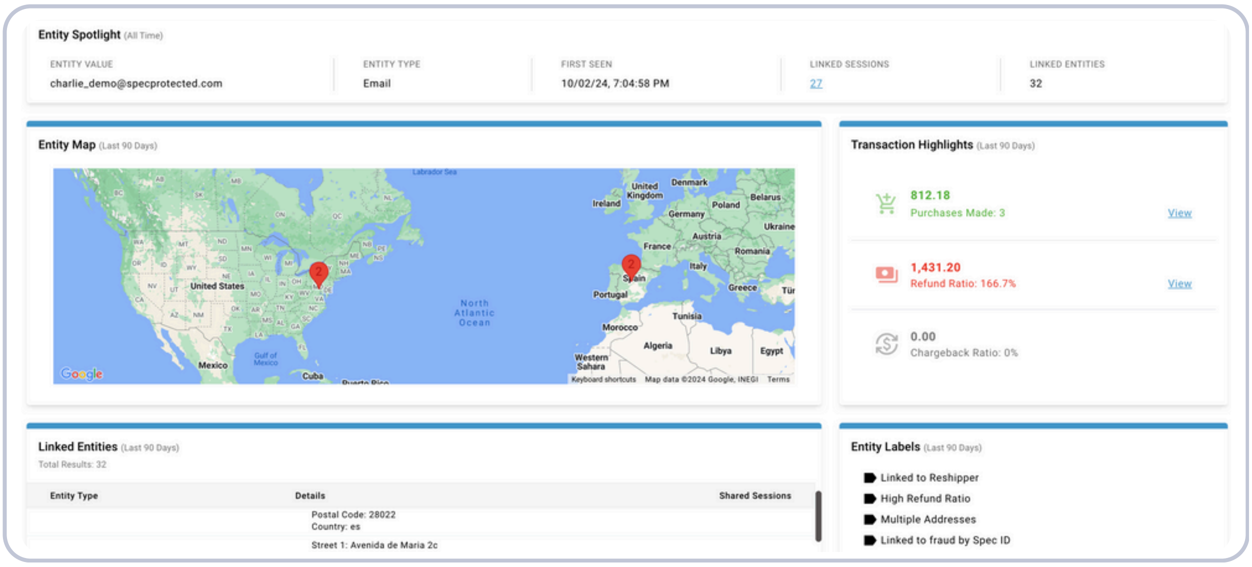
☑ **Unmatched Data Coverage:** Collects 14x more data than traditional fraud tools for deeper insights and broader coverage.

☑ **Proactive and Adaptive Detection:** Uses real-time behavioral analysis to detect and respond to evolving threats before cause harm.

☑ **Invisible Protections:** Secures the customer journey without impacting the experience of legitimate users and customers.

☑ **Easy Integration:** Seamlessly integrates with existing systems, ensuring a smooth deployment process and effortless integration.

☑ **High Accuracy in Risk Decisioning:** Minimizes false positives and operational inefficiencies, providing precise fraud detection.



Entity Spotlight (All Time)

ENTITY VALUE	ENTITY TYPE	FIRST SEEN	LINKED SESSIONS	LINKED ENTITIES
charlie_demo@specprotected.com	Email	10/02/24, 7:04:58 PM	27	32

Entity Map (Last 90 Days)

Transaction Highlights (Last 90 Days)

812.18
Purchases Made: 3
View

1,431.20
Refund Ratio: 166.7%
View

0.00
Chargeback Ratio: 0%

Linked Entities (Last 90 Days)
Total Results: 32

Entity Type	Details	Shared Sessions
	Postal Code: 28022 Country: es	
	Street 1: Avenida de Maria 2c	

Entity Labels (Last 90 Days)

- Linked to Reshipper
- High Refund Ratio
- Multiple Addresses
- Linked to fraud by Spec ID

ATO Fraud Prevention You Can Trust With Spec

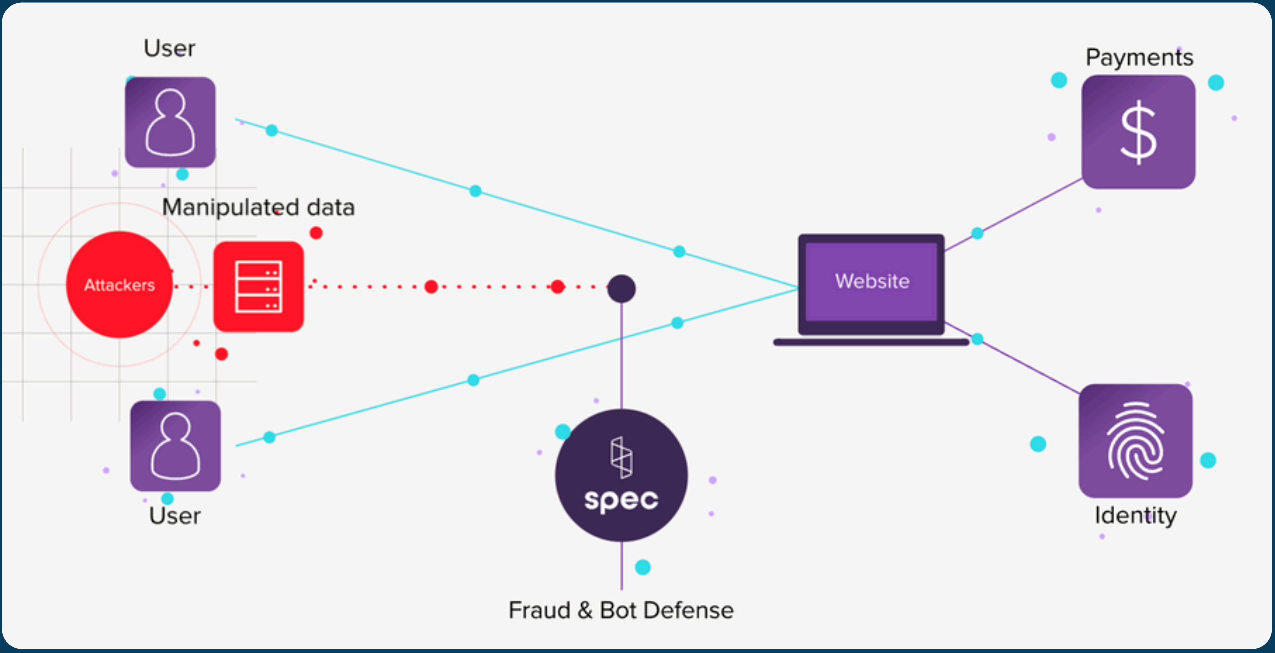
At Spec, we understand trust is essential. That's why the Spec Customer Journey Security platform is engineered with the most stringent security, compliance, and privacy standards in mind.

AICPA SOC · PCI · GDPR · CCPA COMPLIANCE

Spec's platform not only meets industry standards but also ensures a seamless, secure user experience. By adopting an advanced ATO prevention solution, companies stay ahead of sophisticated fraud tactics and safeguard revenue.

Ready to prevent account takeovers?

REQUEST DEMO


User
Manipulated data
Attackers
User
Website
Payments
Identity
spec
Fraud & Bot Defense