How to Defend Against Account Takeover Tactics

The IT Leader's Guide to Preventing ATO Fraud

EBOOK

Table of Contents

What is Account Takeover Fraud?

Account Takeover (ATO) fraud is more than just a cybersecurity buzzword; it is one of the most pervasive threats facing digital ecosystems today. By understanding the fundamental mechanisms and impacts of ATO fraud and its significance in the modern digital landscape, businesses can better equip themselves to effectively prevent and mitigate these attacks.

ATO is a sophisticated cyber attack where malicious actors gain unauthorized access to user accounts to extract sensitive information, financial data, or stored payment methods. These attacks are typically executed through stolen credentials, phishing schemes, or automated bots, often mimicking legitimate users and exploiting security weaknesses to evade detection.

Key Statistics

- **ATO fraud surged by 24% year-over-year in 2024, following a massive 354% increase in 2023.[1]**
- **Identity theft cost businesses and consumers over $635 billion globally in 2023 according to Sift's research.**
- **Average financial loss of $12,000 per incident, underscoring the significant financial and reputational damage these attacks can cause.[2]**

[1] https://sift.com/index-reports-account-takeover-fraud-q3-2024?aliId=eyJpIjoiU3QxV1BmVFZ5aXFKcjh2WSIsInQiOiJXRUxtbDFycXdjTVdndERJcVd3VndRPT0ifQ%25253D%25253D

[2] https://www.security.org/digital-safety/account-takeover-prevention/

The Anatomy of an ATO

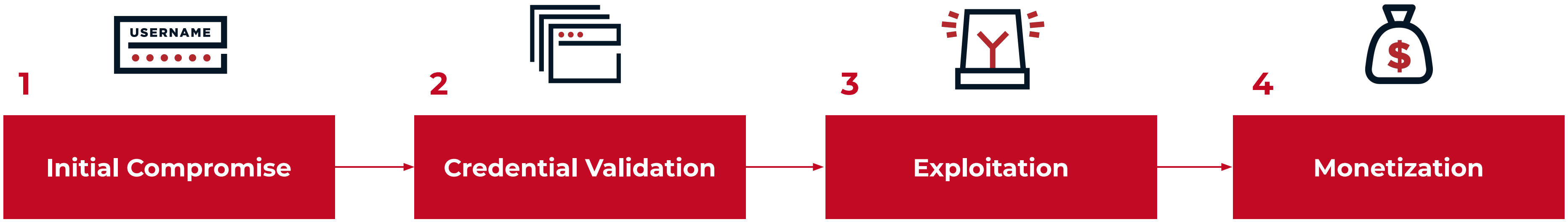
Understanding how ATO operates is key to combating it. Attackers employ a sequence of calculated steps designed to exploit vulnerabilities and avoid detection. By dissecting these steps, organizations can identify gaps in their defenses and proactively address them before damage occurs.

ATO fraud exploits user vulnerabilities and organizational security gaps, following a calculated process that leads to significant financial and reputational harm. Understanding how these attacks unfold is critical for businesses to recognize threats early and implement robust defenses. This chapter dissects the anatomy of an ATO attack to help IT leaders identify and disrupt these tactics.

Red Flags and Indicators of ATO

- **Spike in login attempts from unfamiliar locations or devices.**
- **Multiple failed login attempts in short intervals, indicating brute-force tactics.**
- **Sudden unauthorized changes to account details, such as passwords, recovery email addresses, or phone numbers.**
- **High-volume purchases or unusual account activity.**

An ATO attack typically unfolds in four stages:



1 **Initial Compromise**

Attackers acquire user credentials through phishing emails, social engineering, or purchasing leaked data from the dark web.

2 **Credential Validation**

Bots test credentials across multiple platforms to identify active accounts. This stage often involves credential stuffing or brute-force attacks.

3 **Exploitation**

Once access is secured, attackers modify account settings, make unauthorized transactions, or harvest sensitive data for resale.

4 **Monetization**

Stolen data or funds are sold on dark web marketplaces, used for fraudulent purchases, or weaponized for additional cyberattacks.

ATO's Widespread Impacts

The rapid rise of ATO fraud has made it a pressing concern for organizations worldwide. It's not just the financial losses that make ATO a big deal—the reputational damage and operational strain it causes can have long-lasting consequences, affecting not only the targeted entity but also its customer base. To address this growing threat, businesses must both understand what's at stake and the wide-ranging impacts of ATO, as well as prioritize proactive defense measures.

Impact on Organizations

- **Financial Losses:** Unauthorized transactions, refunds, and chargebacks significantly drain resources. Global ATO-related fraud costs billions annually.
- **Reputational Damage:** Breaches erode customer trust, impacting brand loyalty and customer retention.
- **Legal Risks:** Organizations face regulatory fines and potential lawsuits for failing to adequately protect user accounts and data.
- **Operational Strain:** Increased support tickets and manual fraud reviews burden IT teams.

Consumer Expectations

Ping's 2024 Global Consumer Survey found that **54%** have stopped using an account or online service due to login frustrations, highlighting a growing trend in rising consumer expectations. People across the globe are increasingly less and less willing to accept unnecessary friction in their digital interactions.

Level Up Your Identity Game

Dig deeper into advanced threat protection.

Get the Guide

Industries Under Siege

ATO fraud does not discriminate when it comes to targets. Industries that deal with sensitive data or high volumes of financial transactions are particularly vulnerable, making them prime targets for cybercriminals. Understanding these vulnerabilities can help organizations tailor their defenses accordingly.

Healthcare

Cybercriminals target patient records to commit medical fraud or sell personal health information on the dark web. Advanced email attacks on healthcare organizations, which encompasses ATO, increased by

+167% **in 2023.**[2]

Financial Services

Banking accounts are prime targets for direct fund transfers, fraudulent loans, and identity theft. ATO was up among U.S. financial services companies

+61% **in 2023.**[3]

Retail and Ecommerce

Fraudsters exploit stored payment details, loyalty points, and weak security measures to make unauthorized purchases or resell stolen goods. ATO was up among U.S. retail and ecommerce companies

+54% **in 2023.**[3]

Social Media

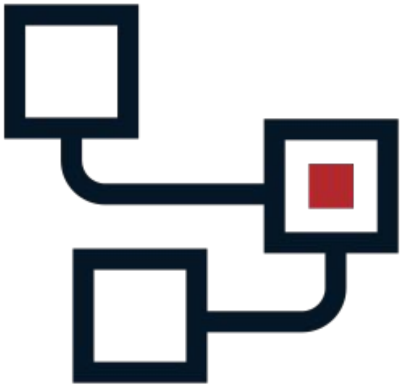
Attackers hijack accounts to impersonate users, spread misinformation, or exploit social networks for financial gain. Social media were the

#1 impacted

type of account in 2023.[4]

[2] https://abnormalsecurity.com/blog/healthcare-organizations-email-attacks-2023
[3] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study
[4] https://www.security.org/digital-safety/account-takeover-prevention/

How Bad Actors Strike: ATO Attack Tactics



Cybercriminals employ a wide range of tactics to execute ATO fraud, often adapting their methods to exploit organizational vulnerabilities and bypass existing defenses. By understanding these tactics, organizations can develop more effective countermeasures and ensure stronger defence against ATO threats.

Automated Attacks

Fraudsters deploy bots to perform credential stuffing and brute-force attacks, testing millions of username-password combinations across multiple platforms.

Stolen Credentials

Leaked credentials from data breaches are used to bypass login security, exploiting users who reuse passwords across sites.

Fake & Tampered Devices

Attackers use device emulators or modify device attributes to bypass security checks, evade detection, and appear as legitimate users.

Session Hijacking

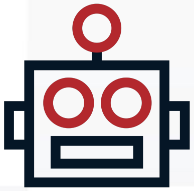
Authentication tokens are intercepted using techniques like Man-in-the-Middle (MITM) attacks, allowing attackers to impersonate users without triggering login alerts.

MFA Bombing

Repeated multi-factor authentication (MFA) prompts overwhelm users, leading them to accidentally approve unauthorized access.

Phishing

Artificial intelligence (AI)-driven phishing campaigns create highly convincing fake emails or websites, tricking users into divulging sensitive information or clicking malicious links.



Tailored Solutions to Defend Against ATO

In combating ATO fraud, generic, one-size-fits-all approaches often fall short. Each organization faces unique challenges depending on its size, industry, and customer base. Addressing the evolving threat of ATO requires a multi-layered defense strategy. Tailored solutions that combine advanced technology with user-friendly practices can significantly enhance an organization's security posture and address the complexities of ATO attacks.

MFA & Identity Proofing

Multi-factor authentication (MFA) adds a critical layer of defense, ensuring that compromised credentials alone cannot grant access. Also consider implementing robust identity proofing tools to authenticate customers during registration, password recovery, and high-risk transactions.

Behavioral Analytics & AI

Leverage advanced AI and ML models to analyze user behavior and detect anomalies such as uncharacteristic behavior and unusual login times, locations, or patterns. Behavioral analytics enables real-time risk scoring, allowing the flagging and mitigation of threats before damage occurs.

Device & Network Analysis

Utilize device fingerprinting and monitor network attributes to identify suspicious devices or IP addresses. Regularly update device profiling rules to stay ahead of evolving attack methods.

Passive & Active Authentication

Passive authentication systems monitor user behavior unobtrusively, while active systems challenge users with secondary verifications when anomalies are detected, creating a seamless yet secure customer experience. Implement a mix of both, stepping up to active authentication methods when risk is high.

Threat-Oriented Orchestration

Centralize threat detection and response with orchestration platforms that integrate various tools, providing a unified view of risks and enabling adaptive responses based on real-time risk assessments.

Preventing ATO: Best Practices for IT Leaders

IT leaders play a pivotal role in safeguarding their organizations against ATO fraud. Implementing a robust strategy to combat ATO requires careful planning and execution. Organizations must adopt a holistic approach that combines implementing robust security protocols, fostering cross-departmental collaboration, and leveraging advanced fraud detection tools, they can mitigate risks and protect both consumer trust and business integrity. The actionable best practices below will enable IT leaders to prevent ATO effectively.

Collaborate Across Departments

Align IT, security, and business teams to implement holistic identity protection strategies

Adopt Robust Security Measures

Combine MFA, identity proofing, and behavioral analytics to create a robust defense, as well as considering passwordless authentication methods.

Centralize Tools

Deploy an orchestration platform to unify your security stack, streamlining detection and response workflows.

Educate Users

Conduct regular training on best practices, including recognizing phishing attempts, using unique passwords, and enabling MFA.

Monitor Continuously

Passive authentication systems monitor user behavior unobtrusively, while active systems challenge users with secondary verifications when anomalies are detected, creating a seamless yet secure customer experience. Implement a mix of both, stepping up to active authentication methods when risk is high.

Threat-Oriented Orchestration

Implement 24/7 monitoring and leverage AI tools for early detection of threats and to adapt quickly to emerging attack vectors

Measuring Success in Fraud Mitigation

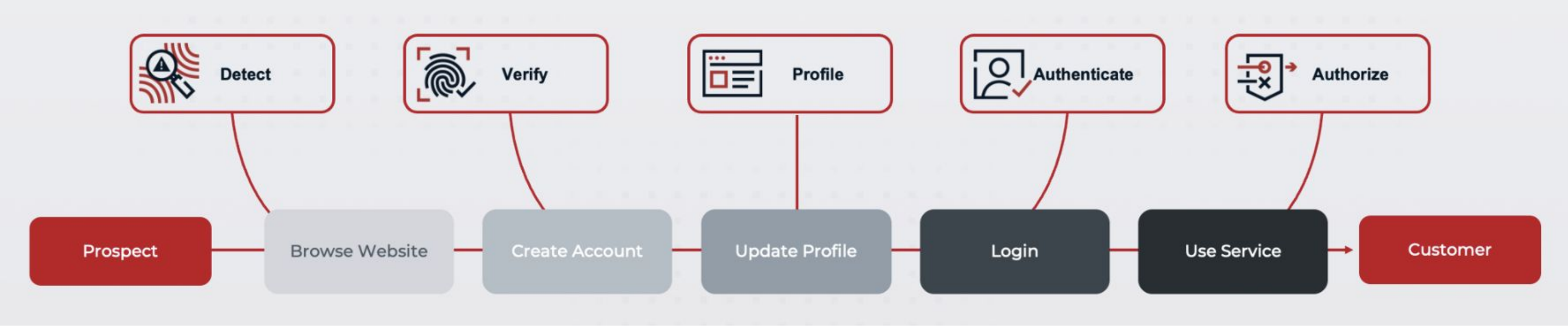
Success in combating ATO fraud requires measurable outcomes. By tracking key metrics and refining strategies based on data, organizations can ensure continuous improvement in their fraud prevention efforts.

Key Metrics To Track

- **Reduction in ATO Incidents:** Monitor the decline in fraudulent activities after implementing advanced tools.
- **Improved Response Times:** Measure how quickly security teams can detect and neutralize threats.
- **Customer Retention Rates:** Monitor customer satisfaction and retention to ensure security measures are non-disruptive.

Tools for Insights

Leverage dashboards and analytics to assess the effectiveness of fraud prevention strategies. Regularly refine policies based on insights gained from threat intelligence.



Graphic 1: Customer identity is foundational at every step in the journey.

Staying Ahead with Modern IAM

Account Takeover Fraud is an ever-evolving challenge that requires constant vigilance and innovation. By combining advanced detection technologies, seamless user authentication, and proactive user education, IT leaders can effectively safeguard their organizations and mitigate threats while maintaining customer trust. Staying ahead demands a commitment to continuous improvement and adaptation to new attack vectors.

Ready to Own Your Identity Strategy?
Develop your threat prevention taxonomy.
Get the Guide

Hear From the Experts

2024 Gartner® Magic Quadrant™ for Access Management

2025 Gartner® Critical Capabilities for Access Management

The Forrester Wave™: Customer Identity and Access Management Solutions, Q4 2024

2024 KuppingerCole Leadership Compass: Passwordless for Enterprise

2024 KuppingerCole Leadership Compass: CIAM

#4105 | 02.25 | v01