THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE

THREE REASONS ATO NEEDS TO BE A PRIORITY THIS HOLIDAY SEASON AND THREE STRATEGIES TO ADDRESS IT

White paper presented by The Fraud Practice

THREE REASONS ATO NEEDS TO BE A PRIORITY THIS HOLIDAY SEASON AND THREE STRATEGIES TO ADDRESS IT

Written by: Justin McDonald, Sr. Risk Management Consultant

A white paper by The Fraud Practice

Sponsored by Sift

Introduction

Account Takeover (ATO) is a major issue with the potential to impact any organization that operates in digital channels and has customers or users who access their site, app or services via a user account login. Risk management strategies have traditionally focused on protecting the payment event, but the proliferation of ATO over the last decade has shown organizations that an effective and robust risk management strategy must cover many events beyond the transaction, to also include account creation, account login and account profile changes.

This white paper focuses on account takeover to specifically discuss why ATO risk should be top of mind for organizations as they prepare final risk management strategy tune-ups ahead of the eCommerce holiday shopping season, as well as provides considerations and strategies for combating this risk. This includes:

Three Reasons Why ATO Should be a Priority This Holiday Season

1. ATO Activity, Like All Fraud, Ramps Up During the Holiday Season
2. ATO Represents Both Direct Fraud Loss and Severe Brand Risks
3. Fraudsters Have all the Data and Credentials They Need

Three Strategies for Addressing ATO Risk

1. Don't Rule Out Using Multiple Solutions
2. ATO is a Dynamic Problem That Requires a Dynamic Response
3. Indirectly Benefit from Your Peers' Experience

Why ATO Should Be a Priority This Holiday Season

Reason 1: ATO Activity, Like All Fraud, Ramps Up This Time of Year

Each year, fraudsters ramp up their activity during the holiday sales period because they know their fraud attempts are more likely to sneak past detection at a time when overall volume is elevated. This applies to ATO fraud in addition to purchase or payment fraud. The peak sales volume and seasonal fraud screening staff are seen as opportunities to professional fraudsters and fraud rings, regardless of whether trying to monetize stolen payment data or compromised login credentials.

ATO jumped 17 percent across Sift's global network during Q3 and Q4 from 2020 to 2021.

Beyond the increased volume and activity the holiday shopping season brings, there are changes in typical buyer patterns that fraudsters exploit as well. During the holiday retail sales rush, merchants are more likely to see and more willing to accept higher priced orders and orders with a shipping address the buyer has not used previously, as it is very common to ship holiday gifts directly to the recipient. These factors work to the advantage of someone with unauthorized account access using stored payment credentials to ship high-priced goods to themselves (or their mules). Fraudsters will gladly pay the gift wrapping fees with someone else's money to make their order attempt appear more legitimate.

More economic uncertainty in 2022 may lead to later holiday gift buying with more orders shipping directly to the gift recipient. Fraudsters who take over an account to use stored payment methods and ship to themselves will blend in with legitimate gift orders.

This has the potential to be a larger problem during the 2022 holiday season than it was the year before. Holiday shopping was pulled forward in 2021 as consumers were concerned with supply chain issues and availability of the gifts they planned to purchase. This year, consumers are facing much more economic uncertainty and are more likely to put off holiday gift buying until later in the season, which may mean more gifts shipping directly to a friend or family member.

There have been notable increases in ATO activity over the past several years with no signs of this trend stopping. According to Sift global network data, ATO activity during Q3 and Q4 increased by 17 percent from 2020 to 2021, while annual ATO fraud grew by 307 percent between 2019 and 2021.

> “Fraudsters target consumer accounts like businesses target potential customers—they’re meeting people where they already are, and putting in the same amount of effort to make a profit. Dormant accounts, or accounts not protected by strong security measures, take less effort to infiltrate. Fraudsters end up with plenty of time to collect credentials, stored funds, and payment information before using it to make unauthorized purchases, or heading back to the dark web to sell the stolen data.
>
> The profits of ATO are attractive for that very reason—they’re not limited to whatever money or points are stored in the compromised accounts. Stolen payment details and login credentials can be used for credential stuffing and card testing across multiple sites, leading to bigger payouts and additional breaches. This is especially true during seasonal transaction spikes and slowdowns, when consumers are spending more money more frequently, or leaving their accounts unwatched for long periods of time. Finally, ATO’d accounts are more valuable than exposed credit card details alone, since the average consumer reuses the same login information across dozens of sites, apps, and services. That's why preventing fraud requires access to real-time insights and adaptable tools that don’t leave analysts chasing after fraudsters, unable to catch up.”
>
> **Jeff Sakasegawa, Trust and Safety Architect at Sift**

Reason 2: ATO Represents Both Direct Fraud Loss and Severe Brand Risks

Organizations tend to focus on the direct financial losses associated with account takeover, which are very meaningful. ATO losses increased by 90 percent in 2021, according to a study from Javelin Strategy and Research[1]. However, organizations must also consider the indirect costs and brand risks associated with ATO, which stems from the fallout among customers or users impacted by ATO fraud and the loss of customer future lifetime value.

42 percent of consumers who fell victim to account takeover had their stored payment methods used for making unauthorized purchases.

According to a consumer survey by Sift[2], 45 percent of ATO victims had money stolen from them directly, 42 percent had stored payment devices used to make unauthorized purchases and 26 percent lost loyalty or rewards points. In each of these cases, the organization that held the consumer account is suffering a direct financial loss as they reimburse the customer or suffer a chargeback, but also consider how this event impacts the victim and their likelihood to continue business with the organization. The same Sift consumer survey also found that 74 percent of consumers will stop using their account if they suffer account takeover on a specific site or app.

Nearly three-quarters of consumers will stop using their account if it falls victim to account takeover.

Can you blame them? It's a major headache for consumers who often become locked out of their account so the fraudster can maximize the value they extract from it. According to a study from Aite-Novarica Group[3], 24 percent of ATO victims have their contact information changed during the ATO incident. Further, ATO is an invasion of privacy, as a consumer's home address, phone number and other information has been exposed to a fraudster.

Sources:

1 - https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults

2 - https://resources.sift.com/ebook/q3-2021-digital-trust-safety-index-battling-new-breed-account-takeover

3 - https://aite-novarica.com/report/us-identity-theft-adapting-and-evolving

Reason 3: Fraudsters Have All the Data and Credentials They Need

When it comes to protecting against ATO, organizations should begin with the assumption that any login credentials may already be compromised. While bot and brute force protection should still be in place, more protection is required. A multitude of risk signals need to be considered to determine when multi-factor authentication or other forms of step-up authentication should be presented to users, even if they provide the correct password on the first login attempt.

Begin with the assumption that any and all login credentials have already been compromised.

Thanks to countless data breaches, compromised email and password combinations are plentiful. We must resign to the fact that consumers are the weakest link in the security chain, frequently reusing passwords. Email or username credentials compromised in a third party data breach will be used against other organizations that may also hold a user account belonging to that data breach victim. Hundreds of millions of passwords are compromised each year and, according a report from SpyCloud[4], 64 percent of passwords compromised in 2021 were reused while 70 percent of passwords compromised prior to 2021 are still in use today.

The Identity Theft Resource Center[5] reported over 53 million data breach victims in the first half of 2022, however, this figure is very likely understated because 39 percent of the 817 reported data breaches did not include a victim count. The hackers aren't stopping, so don't expect ATO activity to abate anytime soon.

Sources:

4 - https://spycloud.com/resource/2022-annual-identity-exposure-report/

5 - https://www.idtheftcenter.org/publication/h1-2022-data-breach-analysis/

Strategies for Addressing ATO Risk

Understanding ATO Risk Exposure

Before discussing the three strategies for addressing ATO risk, it is important to define the concept of ATO risk exposure. Organizations will have different requirements for ATO protection based on their level of ATO risk exposure. Measuring this is a product of the frequency or likelihood of ATO attacks and the severity or level of impact that an ATO event can cause.

Banking and fintech are among the industries with the highest ATO risk exposure. Across Sift's global network, ATO rapidly increased by 850 percent between 2020 and 2021 for fintech firms.

ATO risk exposure varies across organizations but is relative to the type of personally identifiable information (PII) that is stored with, visible or usable from a user's account. This includes factors such as the ability to use a stored payment method once logged in, whether sensitive PII is obfuscated, as well as factors such as password policies, bot checks and other risk mitigation practices at the login event. Other considerations relate ATO protection to payment protection, such as how and when trusted accounts may see reduced fraud screening, and what potential ATO risk signals may lead to that rapport or trust being reconsidered.

ATO risk exposure factors influence how valuable an organization's user accounts are in the hands of fraudsters and help the organization gauge whether their current ATO mitigation strategy is adequate relative to their exposure. ATO risk exposure is highest for financial institutions while there is large variance across merchants contingent on policies, ease of using a stored payment device and visibility into accountholder PII.

Strategy 1: Don't Rule Out Using Multiple Solutions

Payment Protection versus ATO Protection

A robust risk management strategy addresses the entire customer journey – from account creation through purchase as well as subsequent logins and account changes – but effectively designing this often requires the use of multiple solution providers. Risk management for digital channels can be viewed through two lenses, payment protection and ATO protection, with both requiring multi-layered strategies.

Rather than trying to shoehorn all risk management needs through a single solution provider, organizations are often better served by utilizing multiple vendor solutions implemented across different aspects of their risk management strategy. Different service providers have different relative strengths, both across areas of expertise and various vertical markets, and there is benefit in leveraging different service providers at different stages of the customer journey.

There is no silver bullet for fighting fraud and no one-size-fits-all approach.

Historically, fraud solution vendors have placed the most emphasis on payment protection, and many organizations may find themselves effectively using vendors to reduce payment fraud and chargebacks. This vendor may not have an ATO protection service offering, but this doesn't preclude an organization from seeking that out elsewhere. Even if they do offer an ATO protection solution, it may not be the best fit. Organizations should explore all options.

Consider if the vendor is primarily a payment protection solution while ATO protection is a service offering but not necessarily a strength. Organizations with meaningful ATO risk exposure should highly consider solutions designed with ATO protection specifically in mind. Next consider vertical strengths, or whether the vendor is a leader in an organization's industry. For vendors who offer payment protection and ATO protection focused services, the vertical strengths may differ across the two – don't assume they are the same.

Common Pain Point: Using Payment Protection Tools for ATO

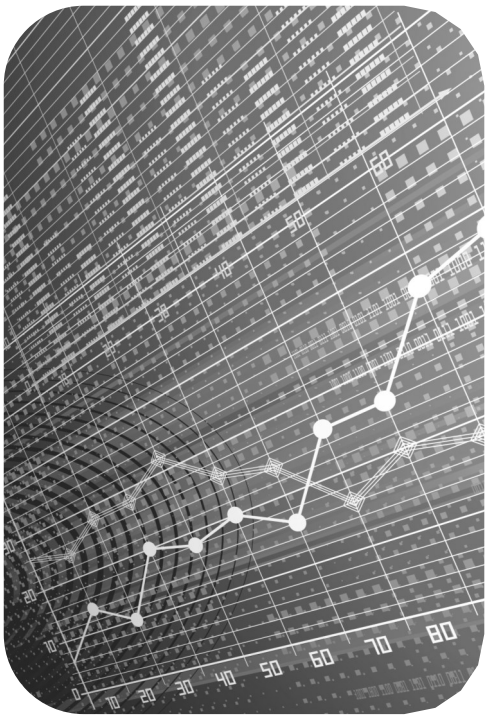
All too often, organizations will do their best to make do with the tools and technology already available to them. Take device identification, IP geolocation and proxy detection for example, which are important tools for detecting ATO when the correct login credentials are presented. When these services are delivered in a way that was built for payment protection, they could be used for ATO protection, but there are a couple of reasons why that may not be the best idea.

Using payment fraud tools for ATO protection can be less effective and more costly.

First, is when these services are delivered or extracted like a tool rather than part of a broader solution. For example, if an organization is just receiving the device ID as a data point, it is up to them to make sense of it. This requires extensive backend development work to collect, store and compare the presented device ID against past user account logins. It is an even greater development effort to take this data and effectively use it for velocity check implementations, such as tallying how many different accounts a given device ID has accessed in the last 24 hours. Building on what they may already collect for payment protection will require significant time and costs to fully utilize, whereas these types of checks are intrinsic with model-based ATO protection solutions (which are discussed more in Strategy 2 below).

Second, organizations need to consider cost. Sticking with the device ID example, when paying a per service call fee, these costs will add up quickly. Device ID services designed for the transaction event are priced as such, but there are many more login events. Organizations that explored using transaction protection-focused services in creative ways for ATO protection likely found it to be cost prohibitive.

Strategy 2: ATO is a Dynamic Problem That Requires a Dynamic Response



Fraud is a moving target. One of the most critical factors differentiating strong versus less effective risk management strategies is the ability to keep up with the constantly evolving nature of fraud and proactively increase protection where it is increasingly needed. In short, a dynamic and adaptive risk management architecture, such as one that is based on modeling, tends to be more effective than a static approach, such as a rules engine that is entirely reliant on analysts and manual processes to keep pace with fraud trends.

This is true in both payment protection and ATO protection implementations. A model-based solution is more adaptive and responsive to changes in trends, both as it pertains to high-risk and low-risk behavior. This leads to quicker pivots that more effectively stop fraud and enable good users to proceed with model-based platforms relative to rules-based platforms.

Machine learning (ML) components to a model-based solution makes it more dynamic yet. They provide an automated way make sense of changing data trends enabling fraud analysts and data scientists to focus more on supervision and testing proposed changes before they are rolled out. Model-based solutions enable more frequent, smaller iterations.

ATO fraud is up 70 percent from the second half of 2021 to the first half of 2022 across Sift's global network.

Rules engines, on the other hand, require an analyst to identify a changing trend, perform analysis to validate it and understand the impact of a rule change, then there are operational steps to edit existing rules or implement new ones. Model-based solutions with machine learning will automate much of this process.

Many organizations see the value of model-based solutions from a payment protection standpoint firsthand, but still take a rules based approach to ATO protection. This is often the result of ATO protection being implemented quickly and reactively out of an immediate need, and understandably so. Rules may have been created to detect risky login activity even when the correct login credentials were provided, such as by comparing the IP address and possibly the device ID to past user logins. These reactionary rules should be viewed as a form of tech debt. They were a needed Band-Aid but are likely not the best long-term solution.

A model-based versus rules-based approach to deciding when to present step-up authentication leads to fewer logins requiring an additional authentication step, which lowers vendor costs and improves UX.

Static, ATO-focused rules are likely to lead to more high-friction logins because fewer signals are considered when deciding to present step-up authentication relative to this decision being made by a more complex model-based approach. There is value in reducing unnecessary step-up authentication, such as two factor authentication. Benefits come both in the form of reducing friction to improve user experience (UX) and cost savings via reduced use of the tools or services used for step-up authentication.

A rules-based approach may always require step-up authentication when there is a new IP address, but a dynamic modeling approach can still find that this is a low risk login. High- and low-risk signals can be identified based on characteristics of the specific login event, and there can be temporary changes in how likely step-up authentication is to occur, such as making it more prevalent during a site-wide attack from a fraud ring or suspicious activity from a specific IP range in the last 24 hours.

Strategy 3: Indirectly Benefit From Your Peers' Experience

Lastly, consider leveraging the benefits of an ATO protection platform that supports cross-merchant data sharing. This broadens the scope of risk models to consider not only patterns specific to one organization, but broader patterns seen across the solution provider's client base. This means an organization's ATO risk scoring models will be able to recognize emerging fraud patterns even when it is the first time the merchant has experienced it firsthand.

Cross-client data sharing works on three levels. First is the recognition of broader fraud trends that influence and improve overall ATO risk scoring. In other words, a merchant may not have seen a new fraud trend yet, but their models are taking this emerging threat into consideration.

Examples of cross-client data sharing include:

1. Identifying trends across clients that influence risk model features or signals for all
2. Shared velocities
3. Shared negative lists

One example may be an increase in blocked login attempts from a given IP range across multiple organizations in the solution provider's network. This would not immediately block all users logging in from this IP range, but temporarily represents elevated risk that would be considered in the model and risk score.

Second is the use of shared velocities. While organizations consider how many times a given data point has been presented, or how many login attempts came from the same IP address in the last hour, without data sharing they are confined to their own data silos. Shared velocities consider use of a data point across a solution provider's entire network.

If a specific IP address has been associated with many blocked logins across multiple organizations in the last hour, data sharing enables another merchant to benefit from this knowledge despite it being the first time that specific IP address was used in an ATO attempt against them. This is also very valuable in recognizing when an email and password combination comprised in a data breach is being attempted against many different organizations.

The third use case for cross-client data sharing that benefits ATO risk protection is the use of shared negative lists. Whereas shared velocities indicate elevated risk, this is one risk signal considered in the context of many, and it may not lead to denying user access or forcing a password reset. For data points to end up on a shared negative list, however, it is confirmed that they are related to fraud or have been compromised.

This could be an IP address that will be blocked at any login attempt across all organizations for the next 24 hours. Another example is leveraging lists of data, such as email and password combinations, confirmed to have been compromised in a breach. Say that several hundred thousand email and password combinations were implicated in a recent data breach and posted on the dark web and there has been a sudden increase in login attempts related to 20 percent of this list. A solution provider focused on ATO protection may add the entire list to a watch list, such that any account using the same email and password combination compromised in the known data breach will be flagged.

There are several factors organizations should consider for assessing and comparing data sharing capabilities and strengths across solution providers, beginning with understanding which of the three use cases discussed above are supported. Merchants should also be careful not to conflate data sharing capabilities across payment protection and ATO protection solutions when providers offer both. Data sharing capabilities may be discussed in a broader context and it never hurts to clarify if something applies to ATO protection, payment protection or both.

Breadth of data and the relevancy of data are also important considerations. In general, the more clients a solution provider has participating in their network, the more ability models have to learn from broader trends and more likely they are to see multiple uses of data points impacting the efficacy of shared velocities and shared negative lists. Relevancy of data refers to the solution provider having many clients in the same or similar industries.

Conclusion

As the holiday shopping season approaches, there is often a tendency to focus on payment fraud, but ATO fraud has been trending upward for several years. The aspects that make this time of year challenging in terms of payment fraud protection also impact ATO fraud, and most (if not all) organizations would benefit from increasing protection on this front as well.

Account takeover is damaging both in terms of direct losses and the indirect losses associated with the immense brand risks ATO represents. Unfortunately, there are no signs of this activity slowing down.

ATO is either a significant problem or has the potential to become one for most organizations. It is critical that organizations understand their ATO risk exposure and consider strategies to mitigate account takeover risk.

Why ATO Should be a Priority This Holiday Season:

1. ATO Activity, Like All Fraud, Ramps Up During the Holiday Season
2. ATO Represents Both Direct Fraud Loss and Severe Brand Risks
3. Fraudsters Have all the Data and Credentials They Need

Strategies for Addressing ATO Risk:

1. Don't Rule Out Using Multiple Solutions
2. ATO is a Dynamic Problem That Requires a Dynamic Response
3. Indirectly Benefit from Your Peers' Experience

Are you looking for answers or solutions, for eCommerce payments and fraud management? Give us a call for a free introductory consultation to see if we can help you. Even if we can't meet your needs we most likely know someone who can, and we are happy to provide you with contacts of reputable firms and individuals servicing the space.

David Montague,
Founder

About the Fraud Practice

The Fraud Practice is a privately held company based in Palm Harbor, Florida. The Fraud Practice provides training, research, and consulting services on eCommerce payments, fraud prevention, and credit granting. Businesses throughout the world rely on The Fraud Practice to help them build and manage their fraud and risk prevention strategies.

For more information about The Fraud Practice's consulting services, please visit www.fraudpractice.com. For additional information about The Fraud Practice's online training programs, please visit www.CNPtraining.com.

The Fraud Practice
www.fraudpractice.com
www.CNPtraining.com
Telephone: 1.941.244.5361
Email: Questions@fraudpractice.com

About Sift

The Sift Digital Trust & Safety Platform empowers companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents fraud and abuse with real-time machine learning that adapts based on our unrivaled global data network of 70B events per month. Global brands including Twitter, Wayfair, and DoorDash rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at sift.com and follow us on Twitter @GetSift.

THREE REASONS ATO NEEDS TO BE A PRIORITY THIS HOLIDAY SEASON AND THREE STRATEGIES TO ADDRESS IT

White paper by The Fraud Practice
Sponsored by Sift