Arkose Labs

Ebook

# Account Takeover Survey

## Top 7 Findings on the Impact of ATO

# Account Protection is Key for Security, Fraud and Identity Teams

Account takeover attacks are the fuel that powers fraud and abuse globally. Personal data from compromised accounts is shared and sold on the Dark Web to then be reused, perpetuating the cycle of every data breach. Money drained from hacked user accounts can be used to fund further downstream scams or to make fraudulent purchases. Legitimate accounts can also be used to send authentic-seeming spam and phishing messages to consumers via email or on a digital platform. There are myriad ways in which ATOs can be used to further the business of fraud.

To find out how businesses are dealing with ATO attacks, Arkose Labs commissioned a market research study polling 100 InfoSec and Fraud executives at U.S. companies ranging in size from 1,000 employees to over 10,000. While most business recognize the negative impact ATOs have on user experience and brand awareness, many were underestimating the amount as well as total cost of ATOs targeting their users.

For businesses that don't have full visibility into the extent of the threat ATOs cause, it is akin to a ship sailing in iceberg-infested waters; everything going along smoothly until disaster strikes and unveils the deep impact looming under the surface. It is critical for all members of the digital commerce ecosystem to work together to quell the threat of account takeover attacks.

Beyond the impact to consumers and the initial cost to businesses, there are many residual problems that successful account takeover attacks cause for companies. These include an impact to brand reputation, negative news headlines and increased regulatory scrutiny.

That's why it is imperative for businesses to focus on protecting the digital front end and stopping ATOs before they happen. Doing so is one of the clearest ways to protect digital consumers and increase trust online.

# 1 Account Security Is The Top Security Concern For Digital Businesses

One thing that is clear is that businesses recognize how important it is to their digital platforms to ensure the integrity of all user accounts. When asked the top three security concerns for their website, more than 70% cited either account takeovers or fake new account registration as a priority. Fake new accounts can be used to send spam and phishing messages to real users in order to extract personal data and information, which can then lead to further ATOs down the line.

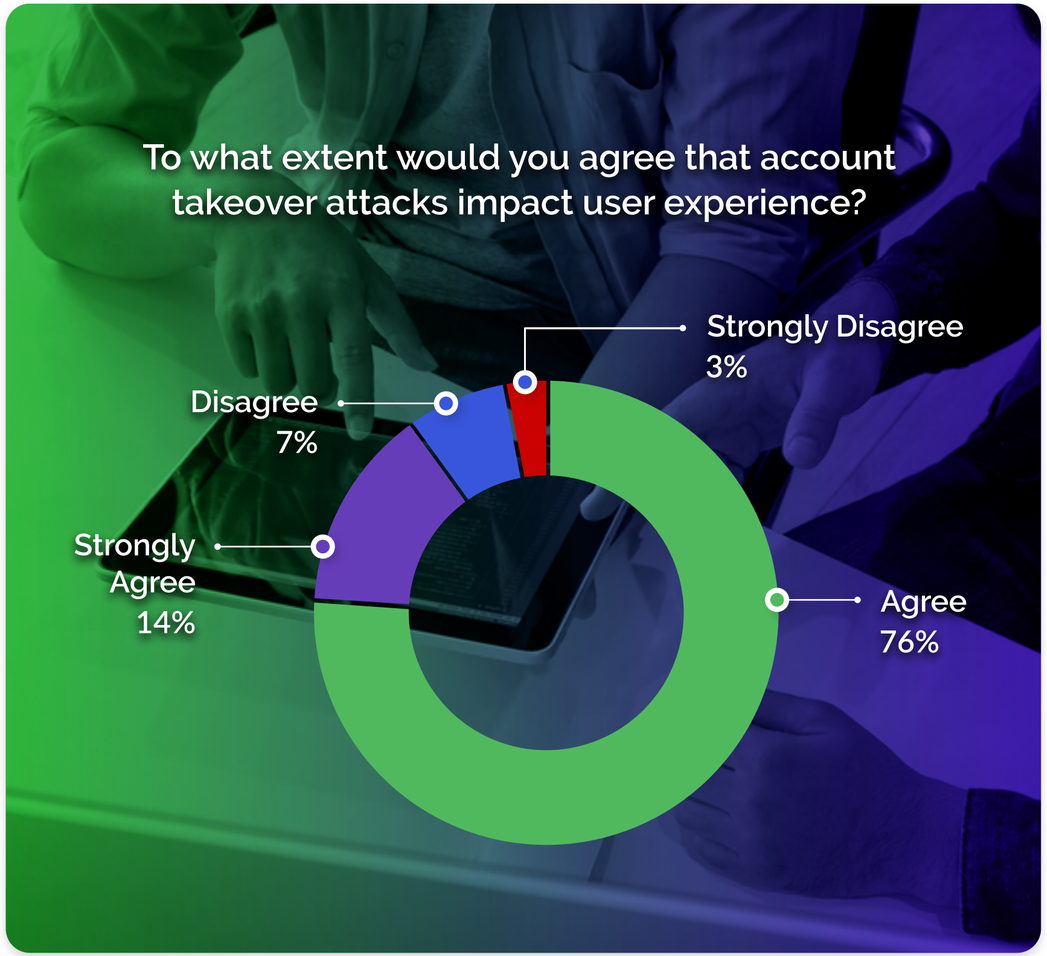
ATOs ranked as a highest concern from respondents in the professional services industry, with 67% citing it as a top issue. That was followed by the healthcare industry, with 44% citing it as a top 3 concern. Simply put, protecting existing user accounts as well as ensuring the integrity of all new accounts created is a major step towards elimianting digital fraud and abuse.

# 2 User Experience Is Front And Center In Account Security

Survey respondents were nearly unanimous in reporting that account takeover attacks severely impact the user experience, regardless of the industry or company size. A full 90% agreed that account takeovers impacted user experience. Even more worrying, about half the companies polled said they had lost customers over the past year due to account takeover attacks.

Think about it from the user's point of view. When an account takeover occurs, people unexpectedly have to deal with customer support reps and spend time waiting while their accounts are restored. Not to mention the anxiety that comes with finding out that their personal data has been compromised and not knowing how that will impact them long-term. Is it any surprise they typically blame the business for not protecting that information?

Businesses must keep customer logins safe and prevent downstream fraud and abuse. However, doing this, without harming user experience can be complex. Security controls, which are too heavy-handed will frustrate customers and send them to competitors. Inaccurate decisioning, which accidentally blocks good users directly, hits the bottom line. Yet, allowing bad actors through and having customers experience fraud on their accounts will also undermine trust.



# 3 ATOs Lead To Compromised Identities And Payment Fraud

Data breaches and hacks that expose consumers' PII are what power the space of account takeovers that digital businesses are dealing with. It's a fact that, if consumer data was never compromised and always kept secure, there would be no ATO to worry about.

Across the overwhelming majority of industries that our poll respondents operate in, compromised identity credentials was cited as the number one negative impact of account takeover attacks, followed by fraudulent transactions, stolen payment details and loss of funds.

Not keeping user accounts safe can also lead to heavy regulatory fines, which all businesses would like to avoid. One European firm was fined more than 200,000 euros by regulators in regards to a credential stuffing attacks that led to hacks of user accounts. In 2015, Dunkin Donuts had to pay a fine of $650,000 stemming from an attacks that breached more than 20,000 user accounts. Keeping user accounts safe can save businesses massive regulatory headaches in the long run. [1]

## The Most Significant Impacts of Account Takeovers to End Users:

**40%**
Compromised Identity Credentials

**32%**
Fraudulent Transaction

**14%**
Stolen Payment details

**8%**
Loss of funds

**3%**
Time spent to reclaim account

**3%**
Other

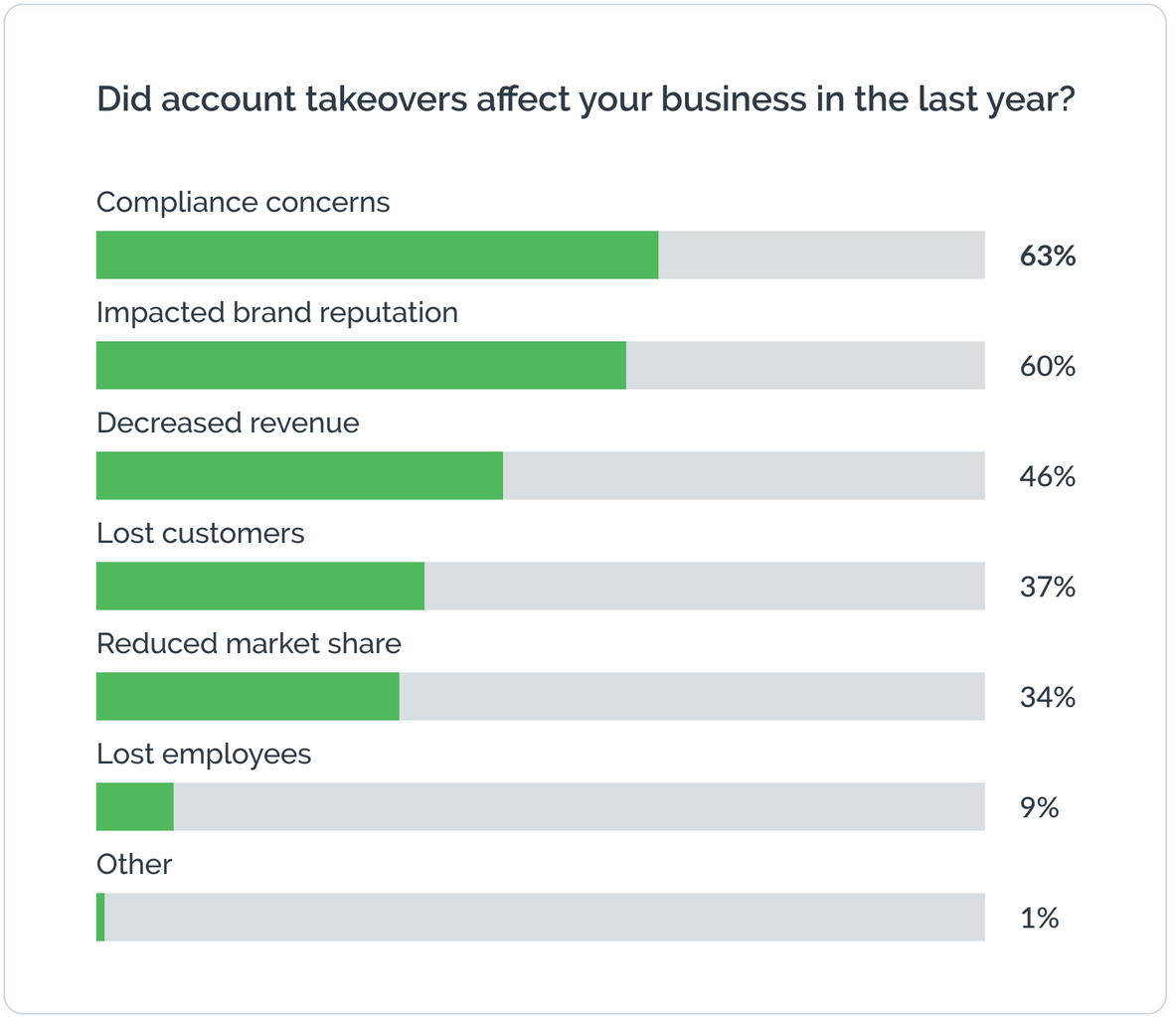
[1] *https://ag.ny.gov/press-release/2019/ag-james-sues-dunkin-donuts-glazing-over-cyberattacks-targeting-thousands*

# 4 Top Business Impacts Of ATOs Are Compliance And Brand Reputation

Besides the immediate costs associated with ATOs, there are many downstream costs as well. One that is often most unexpected is the an impact to brand reputation. Users who have accounts compromised are much less likely to remain long-term customers. They also will go on social media platforms to express their unhappiness, thus amplifying the negative brand message.

Compliance concerns are another big problem associated with account takeover attacks. If a businesses allows it' users accounts to be successfully attacked at scale, it will draw the attention of regulators, who will then start asking difficult questions about the security or lack thereof of their platform. This is turn leads to greater compliance costs and burdens on internal teams.

Financial services firms were among the most likely to report a negative impact to both brand reputation and compliance as a result of ATOs. 72% reported that ATOs affected brand reputation, and 66% said ATOs created compliance concerns, both larger than the cross-industry average.



# 5 Responsibility For Account Security Is Spread Across Internal Teams

One interesting result from our survey was that the responsibility for handling and preventing ATO attacks varied somewhat. While the majority of those polled said that it fell in the realm of information security, other companies put ATO responsibility in the fraud, engineering or product departments.

This was especially true for larger companies (more than 10,00 employees), where only 55% said information security handled ATOs, followed by fraud 29%, and engineering at 14%.

With impacts on compliance, brand reputation, decreased revenue, and lost customers, ATOs are not simply a security problem; they're a business problem.

For any size company, it is vital that ATOs are handled centrally and a dedicated team is assigned to it, due to the severe negative impact they can have on business growth.

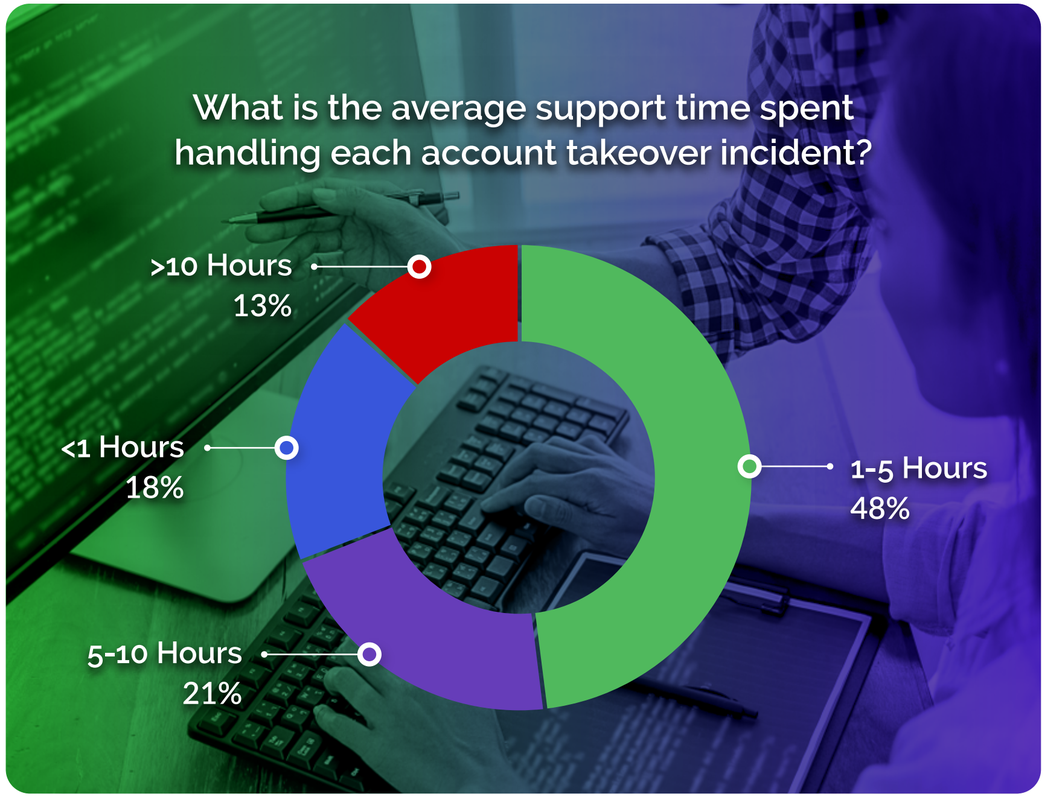
# 6 Ineffective Account Security Is A One-Way Ticket To Efficiency Bottlenecks

Handling and remediating every single successful ATO attack is very time-consuming for businesses - an average of 1-5 hours per incident. Reducing the amount of successful ATOs would allow businesses to operate much more efficiently.

Even spending one hour of support time handling each incident can lead to thousands of wasted hours per month. This includes calls to overworked call centers, increased manual reviews from internal fraud teams, impacts on product and customer acquisition and even increased workloads for legal and compliance departments.

Steps typically implemented by businesses don't always help the problem. Multi-factor authentication, for example, is costly to businesses and created unneeded friction to users, forcing them to take extra steps to authenticate. When consumers are inadvertently locked out of their accounts when they fail authentication steps this dramatically adds to the operational burden of account security.

Businesses need intelligent authentication strategies that reserve step-up authentication only for users presenting with risky attributes, and should consider self-remediation options that screens traffic while avoiding blocking good users.

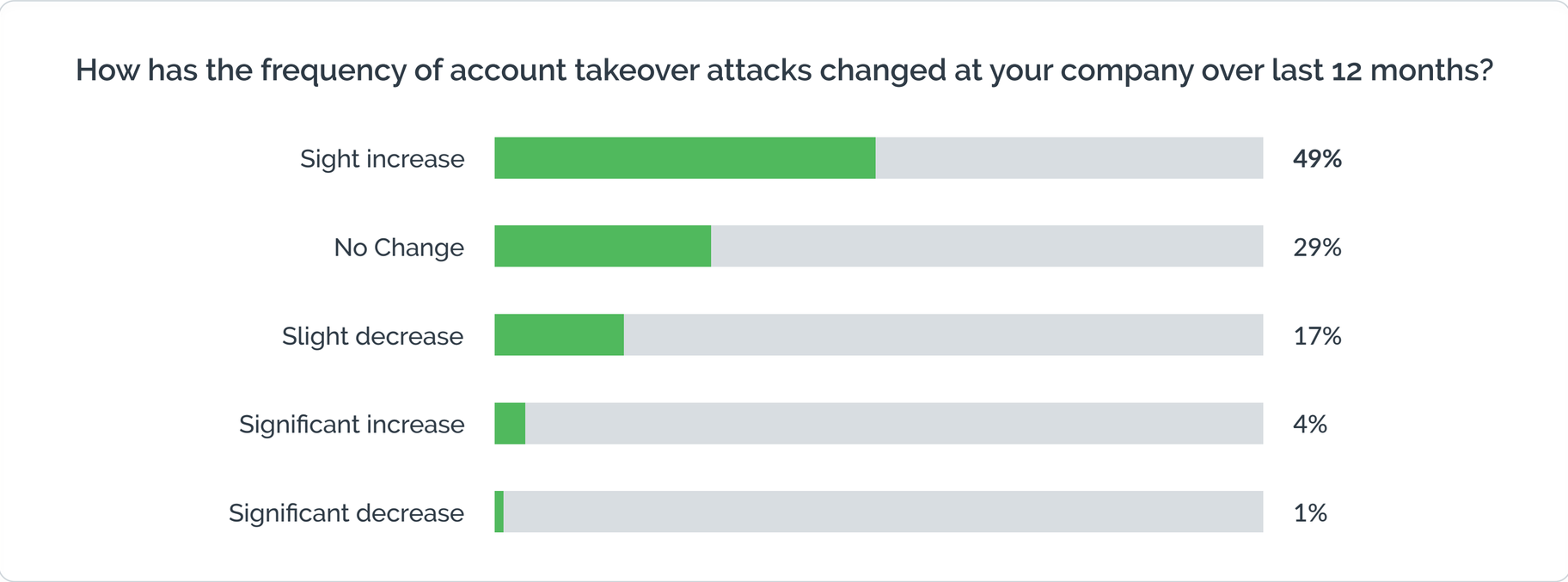


# 7 The Full Volume Of Account Takeovers Is Being Missed

Nearly half of the companies we polled reported only a slight increase in ATO attacks in 2020, and nearly 30% said there was no increase. This could indicate that businesses are not getting full visibility into the volume of attacks targeting them. By contrast, the Arkose Labs global network recorded a significant increase in attacks on logins, with automated credential stuffing attacks being a key driver of volumetric attacks

.

Lack of visibility into ATO attacks is not uncommon among businesses; ATOS are not always immediately obvious and often only discovered after downstream abuse is detected. For example one Arkose Labs client was seeing 30,000 account takeover attempts per day, the vast majority of which they were unaware of before implementing the Arkose Labs platform.



# Account Security Strategies for Digital Businesses

Compromised accounts can lead to an array of downstream disruption - for both users and businesses. ATO attacks lead to stolen money, assets and loyalty point; spam and scams targeting good users, and downstream payment fraud. Ineffective account security will add to operational costs, as fraud and security teams will have to more closely monitor traffic and customer support personnel deal with an increase in customer complaints.

Many companies, however, do not have the luxury of implementing stringent security controls that can frustrate good users while trying to slow down fraudsters. This is because it can lead to decreased revenues.

For this reason, digital businesses need preemptive insight into malicious activity on their platforms, which is based on real-time risk assessments and anomaly detection driven by machine learning. In a world of increasingly inconclusive signals, however, they also need an attack response strategy to interdict high-risk traffic. When combined with sophisticated risk detection, a highly targeted challenge-response strategy can be the best route to confidently identifying account takeover attacks.

# Arkose Labs for Account Security

Global brands trust Arkose Labs to detect and deter attacks at user authentication touchpoints where account takeover, fake account creation, bonus abuse, inventory hoarding, and scraping originate. By rooting out fraud early in the customer life cycle, you'll reduce stress on the payment flow and have greater confidence that it's a real customer on your platform.

## Solving the False Positive vs False Negative Conundrum

Arkose Labs' AI-powered platform combines real-time risk assessment with dynamic attack response to defeat persistent bots and co-ordinated human attacks on the most targeted user action points on websites and apps. Invisible risk assessments allow good users to pass through seamlessly. High-risk traffic is triaged for active attack response that deters future attempts and creates a more secure experience for genuine customers.

## Comprehensive Protection Across the Digital Front-End

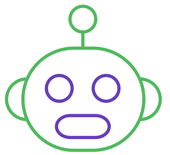

Account Takeover


Credential Stuffing

Fake Account Registrations


Loyalty Point Theft


Bonus Abuse



Bot Attacks

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a “Cool Vendor in Fraud and Authentication,” the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput. Based in San Francisco, CA with offices in Brisbane, Australia and London, UK, the company was honored as the 195th fastest growing companies in the United States on the 2021 Inc. 5000 list.



***Offices***

**San Francisco**
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

**Brisbane**
315 Brunswick St, Brisbane,
Queensland AU

**United Kingdom**
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Schedule Demo