sift

Q3 2020 DIGITAL TRUST & SAFETY INDEX

Account Takeover Fraud and the Growing Burden on Business

Contents

Account Takeover Fraud: E-commerce's Catch-22

Consumers think about fraud differently than businesses do. They're concerned about things like identity theft and social media scams, or having their credit card information stolen when making an online purchase—but they tend to think of these risks as relative to the sites, apps, and businesses they interact with, and how trustworthy they consider those sites to be. If someone opens a new bank account with a major financial institution or signs up for a service from a reputable brand, they expect those accounts and transactions to be secure, and for those merchants and apps to protect their data. But when a fraud vector is as pervasive and scalable as account takeover (ATO), businesses struggle to keep up with consumers' expectations for a safe, streamlined experience.

Account takeover's threat is inarguably big—according to a recent study, total identity fraud losses reached $16.9 billion in 2019—but the financial impact to consumers isn't the whole story. The study also indicates that digital criminals are "targeting smaller numbers of victims [while] inflicting damage that is more complex to prevent or remediate."

% change in ATO rate between Q2 2019-Q2 2020

In fact, ATO rates skyrocketed by **282%** between the second quarter of 2019 and Q2 2020. This astronomical jump represents the percentage of total logins across the entire Sift global network that were stopped because they were fraudulent.

Although this number is alarming, it's not surprising. The internet's rapidly evolving ATO fraud problem has been a primary pain point for businesses over the past decade—a period of such enormous technological innovation that it's led to almost as many structural breakdowns as it has breakthroughs. More recently, entire markets have been reimagined by digital-first businesses that were early to recognize where the world was heading: towards a consumer base that seeks out convenience, customization, speed, and security.

Long before the pandemic made it necessary, these shifting demands produced solutions to serve them: mobile ordering, one-click checkouts, on-demand streaming, and subscription services for almost anything we could dream up. Naturally, these solutions were barriers that a new generation of fraudsters wanted to break through. To adapt to consumers who are both aware and wary, they developed more sophisticated strategies to specifically exploit e-commerce and the consumers who depend on it. Fraudsters who specialize in ATO are efficient; they attack at scale, using automated bots to enter stolen account data or scour the web for information to help them crack security codes and questions.

Fraudsters' determination to bypass account security checks puts merchant risk teams in a tight spot, creating a seemingly endless catch-22 between fraud and friction. Companies want to give customers the streamlined experiences they demand, but to deal with evolving account takeover, are forced to interrupt the user journey with security hurdles:

- Two-factor authentication (2FA)
- Biometrics
- Multi-factor authentication (MFA)
- Single-use passwords
- Captcha codes
- Verification by manual review
- Limited login attempts

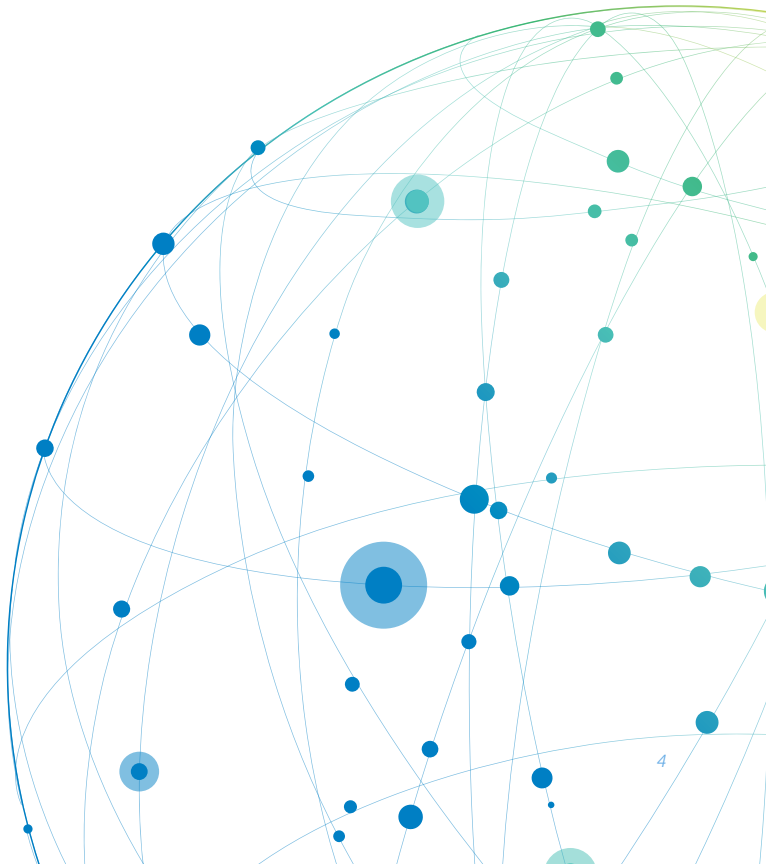
It's an exhaustive list, filled with gates that fraudsters constantly try to dismantle, and that mangle the customer experience. As frustrating as this neverending digital fencing match might be, with fraudsters and risk teams dodging and parrying back and forth, the real problem isn't that e-commerce companies need to keep adding blockers for fraud. It's that they need to add smarter ones that can keep up with the scope and scale of ATO, without jeopardizing consumers' interaction with a brand.

Businesses often depend on users to do the work of verifying themselves through multi-factor authentication or biometrics, providing additional friction for users, and more points of entry that fraudsters can take advantage of. Forcing users to repeatedly prove they're who they say they are causes frustration for them and cart abandonment for businesses. It can also contribute to higher false-positive rates when customers struggle with barriers, unintentionally appearing suspicious if they've forgotten a password or fumbled a biometric scan.

Internally, trust and safety teams are expected to walk an inflexible line while shouldering the burden of manual review; if they block too many orders, they've lost legitimate revenue. When they block too few, they find themselves drowning in chargebacks. Nobody wins—except the fraudsters who manage to sneak past rigid rules, the fraudsters who have enough info to pretend they're someone else, and the fraudsters who get through risk teams overwhelmed by manual review.

The data in this report is derived from the Sift global network of customers, representing over 34,000 sites and apps across all e-commerce verticals, in addition to a survey of over 1,000 consumers* conducted in August 2020. These combined insights give online merchants direct visibility into why, how, and when account takeover fraud can disrupt a business, along with actionable steps merchants can take to consistently treat fraudsters how they should be treated—and deliver the quick, easy, and secure experiences that customers deserve.

**On behalf of Sift, Dynata polled 1,000 adults across the United States via online survey, age 18+, in August, 2020.*



Insights From the Other Side: When Consumers Face ATO

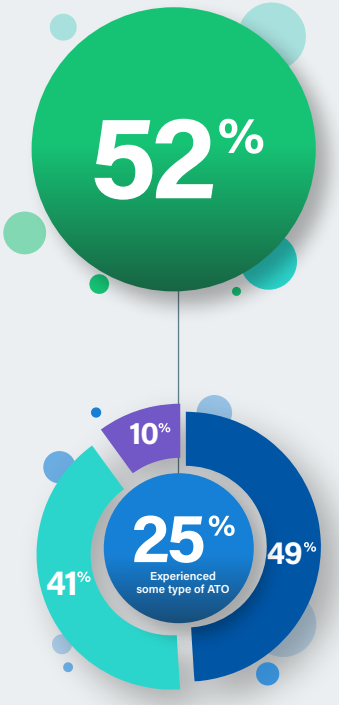
ATO's seemingly unstoppable growth is daunting; since 2018, the number of stolen credentials for sale on the dark web has spiked by 300%. But e-commerce businesses must come to terms with a critical truth: **consumers expect merchants to protect them from fraud**. Consumers assume that the sites and apps they're making purchases on are secure, and that sharing their data and payment details won't come back to haunt them. They believe that safe transactions are a given, that the goods or services they've bought will be delivered, and that the shopping experience will be fast and seamless.

But often those expectations are shattered, either by friction or by fraud, and most consumers aren't taking the time to fortify or keep tabs on their own credential and device security. We found that **two-thirds of consumers** surveyed* either don't use any type of password manager or aren't sure if they do, despite **over half of them** having concerns about becoming victims of ATO in the future.

The worry is valid; **one-fourth** of consumer respondents have already experienced some type of account takeover fraud, and of those victims, **10% have had it happen more than five times**. Nearly half of victims have faced account takeover at least once, and **well over one-third of them** have had it happen between 1-5 times.

Account Takeover in Numbers

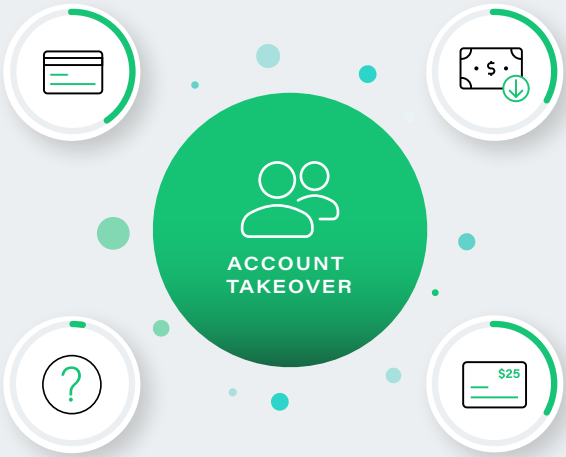
We asked consumers if they've ever been a victim of account takeover, and their responses paint an unfortunate picture: one-fourth of participants have already experienced ATO and dealt with its repercussions (in some cases, multiple times)—and over half are concerned about their personal accounts being compromised in the future.



- **52%** of respondents are concerned about ATO happening to them in the future
- **25%** of respondents have experienced some type of ATO
- Of consumers who have had an account hacked, **49%** had it happen once
- Of consumers who have had an account hacked, **41%** have been victims between 1-5 times
- Of consumers who have had an account hacked, **10%** have been victims more than 5 times

ATO's Role in the Fraud Supply Chain

Fraudsters' specific tactics may change with the target, but more often than not, the end goal is some type of financial gain. Recent research conducted by Sift surfaced a deep interconnectivity among different fraud vectors, including where they fit into the "fraud supply chain" and how these different attack types can facilitate payment fraud. When we asked victims of ATO what happened after their accounts were hacked, their responses further supported those findings.



My stored credit card or other payment type was used to purchase items on the website or app on which I held the account: **41%**

Money was taken out of my account: **37%**

Rewards points/credits were taken out of my account: **37%**

Other/unknown: **2%**

For consumers who've gone through the hassle and repercussions of ATO, righting the wrong went beyond changing a password. Recent research from Sift shows an undeniable interconnectivity between fraud vectors, and demonstrates how different attack types enable payment fraud. Consumer data bolsters those discoveries—after hacking victims' accounts, the actions fraudsters took next make it clear that their primary motivation is financial gain.

Payment details were stolen and used to make purchases in **nearly half** of cases, and **over one-third** of victims had money taken directly from their accounts. Another **37%** had rewards points or credits taken and used to buy goods and services.

People can end up on the path to account takeover virtually anywhere. Victims of ATO reported that their credentials were compromised on a full spectrum of sites, from online dating to travel, streaming services, delivery, and banking, with **over one-third** of respondents attributing account takeover to their activity on social media. This number is especially daunting considering that the average person spends about two-and-a-half hours perusing social accounts each day, giving them plenty of exposure to potential fraud.

Over one-third of respondents fell victim to ATO after interacting with digital e-commerce sites; another third had their financial services accounts compromised. Online dating, which is rife with romance scams, led to account takeover for nearly one-fourth of victims; **almost one-fifth** had their credentials hacked on travel sites, and a small but significant percentage became victims via on-demand/delivery services.

Consumers Are Constantly at Risk

Consumers aren't ignorant about the dangers of account takeover, and when we asked those who've experienced ATO where their credentials were hacked, social media and digital e-commerce sites topped the list. But the rest of the internet is cause for concern, too, with fraudsters finding victims everywhere—from financial services platforms to food delivery apps and dating sites.

36% Social media

36% Digital e-commerce (websites/apps on which you buy streaming services, games, or other digital products/services)

35% Financial services

25% Physical e-commerce (websites/apps on which you buy physical products, e.g. Poshmark, Amazon)

22% Online dating

19% Travel

12% On-demand + delivery services (includes meal delivery, ridesharing, freelance labor services)

8% I'm not sure or do not know which accounts were taken over

7% Work apps/sites (e.g. Slack, Microsoft)

Coupled with industry insights on password hygiene—including that 62% of people surveyed by LogMeIn reuse passwords for both work and personal accounts, and 65% reuse the same password for multiple or all of accounts they own—it seems likely that most consumers will at least become a hacker's target, or be defrauded by ATO at some point. And while it's always possible for individual users to adopt stronger security measures, more complex passwords, or a regular routine for updating credentials, the data shows that most people don't take it entirely upon themselves to keep their digital information safe. This is true even for some consumers who have already faced fraud: of ATO victims surveyed, **12%** reported that they would take no action to further secure their data post-account takeover, and one-fifth of respondents would simply contact customer service to report the issue, without taking additional actions to improve their account security.

These findings reveal that customers depend heavily on merchants to protect them from fraud. Yet when we asked victims of account takeover how they discovered they'd been hacked, **just under half of them** said they found out on their own after logging into the account and noticing suspicious activity, while only **about one-third** were proactively notified by the site or app where the fraud occurred. While not conclusive, this suggests that some merchants are not closing the loop on fraud, which could lead to negative consequences for businesses and buyers alike.

This misalignment between customers' assumptions about who's responsible for their online security, and merchants' ability to provide widespread protection, is precisely the type of loophole fraudsters can use to orchestrate account takeover at scale. Trust and safety teams can only do so much manual review before experiencing decision fatigue, insulting legitimate customers, or failing to stop fraudsters from sneaking through anyway. When these things start to happen, the impact on consumers is clearly significant—but the impact on merchants can be devastating, and even permanent.

**On behalf of Sift, Dynata polled 1,000 adults across the United States via online survey, age 18+, in August, 2020.*

Communication Gap: 62% of ATO Victims Weren't Alerted by Merchants

Fraudsters will exploit any security weaknesses they discover, and in an ideal market, both consumers and merchants have effective tools and practices in place to stop them. But when we asked victims of ATO how they'd learned their information had been compromised, only about one-third of victims reported that they were proactively notified by the merchant, with the remaining 62% left to learn they'd been defrauded after the damage had already been done.

- I logged into my account and noticed suspicious activity: **43%**
- I was notified by the website/app where I held the account: **38%**
- I was notified by my credit card/ financial services company that my payment information had been used to make suspicious purchases: **18%**
- Other: **1%**

The Creeping Cost of Account Takeover

All fraud undercuts revenue, but ATO has wiped out billions of dollars from businesses and consumers over just the past few years. Its scalability and repeatability as a fraud vector make it an ideal weapon for digital criminals, especially if they're adept at using bots or sophisticated malware to execute attacks.

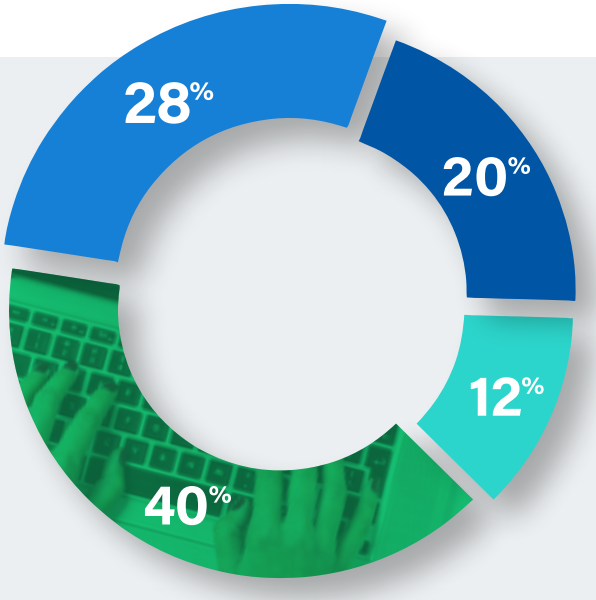
The profits of account takeover are attractive because they serve the dual purpose of getting a fraudster closer to a financial payout and potentially expanding their collection of stolen credentials. This makes online accounts more valuable than stolen credit card details alone, because the average consumer uses about 191 sites or services that require a username and password, and about **62%** use the same credentials across multiple websites. A single stolen password can give fraudsters access to a complete online identity, making them appear legitimate and enabling them to compromise accounts associated with that identity. And if hackers were only after one account at a time, ATO might not be such an enormous problem—but they're not targeting individual sets of credentials one after the other. They're targeting millions of them at once.

In February 2019, TechCrunch reported that a hacker, who had previously stolen approximately 620 million user records from across 16 websites, had done it again. This time, he hijacked 127 million more records from eight additional sites. That means that nearly 750 million user accounts were compromised by a single, savvy fraudster who found security weaknesses on just 24 separate websites. The possible damage becomes intimidating when we consider how many websites exist on the internet, and that no one knows exactly how many cyber criminals are currently active.

The Hidden Cost of ATO: Churn and Chargebacks

Account takeover causes even loyal customers to distrust the websites where their information has been compromised, hurting overall brand loyalty, profits, and long-term growth. When we asked consumers how they'd respond to an account they owned being hacked, **nearly one-third of respondents said they'd stop using the impacted site or service and turn to a direct competitor.**

Similarly, ATO can lead to a major uptick in chargebacks (e.g., charges that are returned to a payment card after a customer successfully disputes a purchase). Recent Sift network data shows that e-commerce ATO rates rose by **282% last year**, and external research found that 57% of businesses experienced increased losses associated with account opening and account takeover in 2019. With around 30% of customers having filed chargeback claims in 2019 due to purchases being made with a stolen account or payment card, the connection between chargebacks and ATO is a formidable issue for all e-commerce merchants. It's also worth noting that "sleeper accounts" can come back to bite businesses down the road—if the 12% of consumers who would not change their behavior were to leave their hacked credentials as-is, ATO can happen to that same account in the future.



- Keep using the site/service, but change credentials/personal info: **40%**
- **Stop using the site or service and select another provider: 28%**
- Keep using the site/service, and contact support: **20%**
- No change in behavior: **12%**

For merchants, preventing account takeover is a smart financial move, since it's directly linked to two of the most expensive fallouts a business can face: brand abandonment and chargebacks. Brand abandonment can be loosely measured in terms of, an average customer's cart value, but the total damage done when someone leaves a business behind can't be quantified. When we asked consumers how they'd respond to becoming a victim of ATO while using a website or app, **over one-fourth of them said they'd take their business to a competing brand or service, never to return**. If merchants consider lost sales in the context of the average customer's lifetime value (LTV), as well as customer acquisition costs (CAC), the consequences of account takeover get exponentially bigger—and even the most accurate data doesn't account for the impact of negative reviews, or someone actively discouraging others from frequenting a business.

Chargebacks can present an even costlier challenge for e-commerce businesses. In 2019, approximately 30% of chargeback claims were filed due to questionable purchases being made with the claimant's stolen account or payment card. Overall, they cause significant financial loss, waste a lot of time and resources, and are even more complex to fight because they can come from both fraudsters and trusted customers. Last year, chargebacks (including friendly fraud) were responsible for about 75% of e-commerce fraud losses. They're also one of the most common results of any account takeover that's used to buy goods with stolen card info—once the fraud has been discovered, it's a safe bet that no customer is going to eat the cost of unauthorized charges.

COVID-19 and ATO: A dangerous duo

The strain that ATO puts on merchant risk teams can become quickly overwhelming, because these teams are usually held responsible for losses that occur as a result of fraud. After all, it's a trust and safety team's responsibility to understand how fraudsters operate, and to prevent or mitigate fraud whenever it surfaces. This strain became even greater as the COVID-19 pandemic spread. The massive disruption coronavirus caused for e-commerce businesses has rendered predictability and playbooks largely irrelevant; risk teams are now fighting fraud in the face of unexpected shifts in market demand and erratic consumer buying behaviors.

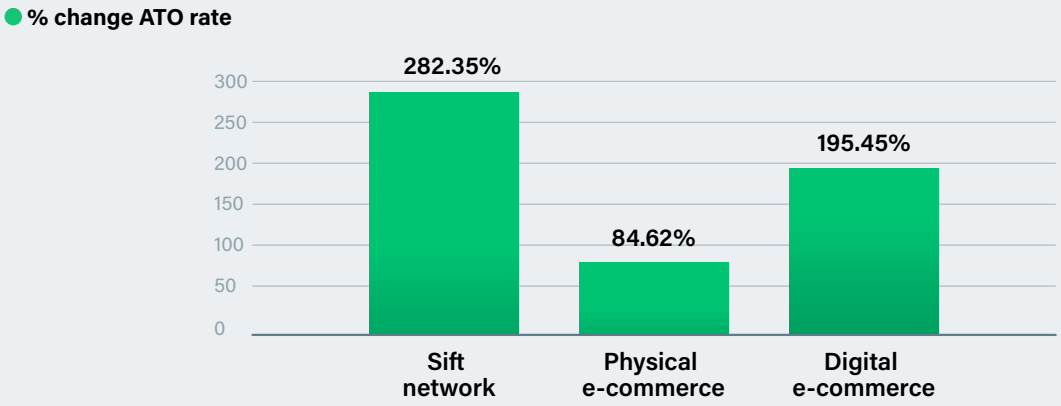
No vertical has been impacted by rising account takeover and pandemic-era disruption like physical e-commerce, which saw a **378.26%** jump in ATO rates between March and August 2020. BOPIS (buy online, pickup in store) and BORIS (buy online, return in store) transactions have become much more common, giving fraudsters expanded opportunities to exploit physical e-commerce businesses. For those that are forgoing the usual verification steps (e.g., scanning an identification card or payment card at pickup) in order to minimize person-to-person interactions, it's especially difficult to stop fraudsters from placing orders online using stolen credit cards, and then picking up their purchases at a physical location or having them shipped to a new address.

Without tools and processes that are capable of adapting and scaling with changing fraud, and preventing fraudsters from exploiting vulnerable points in the customer journey, merchant risk teams will forever be lagging behind. Businesses lose money and credibility with every attack, while consumers are either left to face multiple levels of friction or risk with every online purchase.

E-commerce Account Takeover 2019-2020

Top Targets: The Year-Over-Year Impact of ATO

Account takeover has been one of the most pervasive forms of fraud since the dawn of online business, and the past few years have shown that it's the average fraudster's weapon of choice. The below graph represents the percent change from Q2 2019 to Q2 2020 for overall ATO rates (the percentage of total logins that were stopped because they were fraudulent). Data is illustrated for the entire Sift network, and individually separated out for physical e-commerce and digital e-commerce.



COVID-19 Fraud: Impact of ATO on Physical E-commerce March-August 2020

Since the start of quarantine, the rampant spread of COVID-19 has driven attempted ATO fraud especially high for physical e-commerce businesses, which sell tangible goods to online customers. Many merchants with a small or nonexistent online presence pre-pandemic have pivoted dramatically in order to stay afloat, attempting to quickly scale operations to meet increased digital demand.

Additionally, BOPIS (buy online, pickup in store) and BORIS (buy online, return in store) have become typical in a pandemic-era marketplace. This click-and-collect process lets fraudsters exploit physical e-commerce in the same way they've exploited online merchants for years: by using a stolen credit card, placing an order online, picking up the goods at the store, and either keeping the items, returning them for store credit, or reselling them for profit.

sift

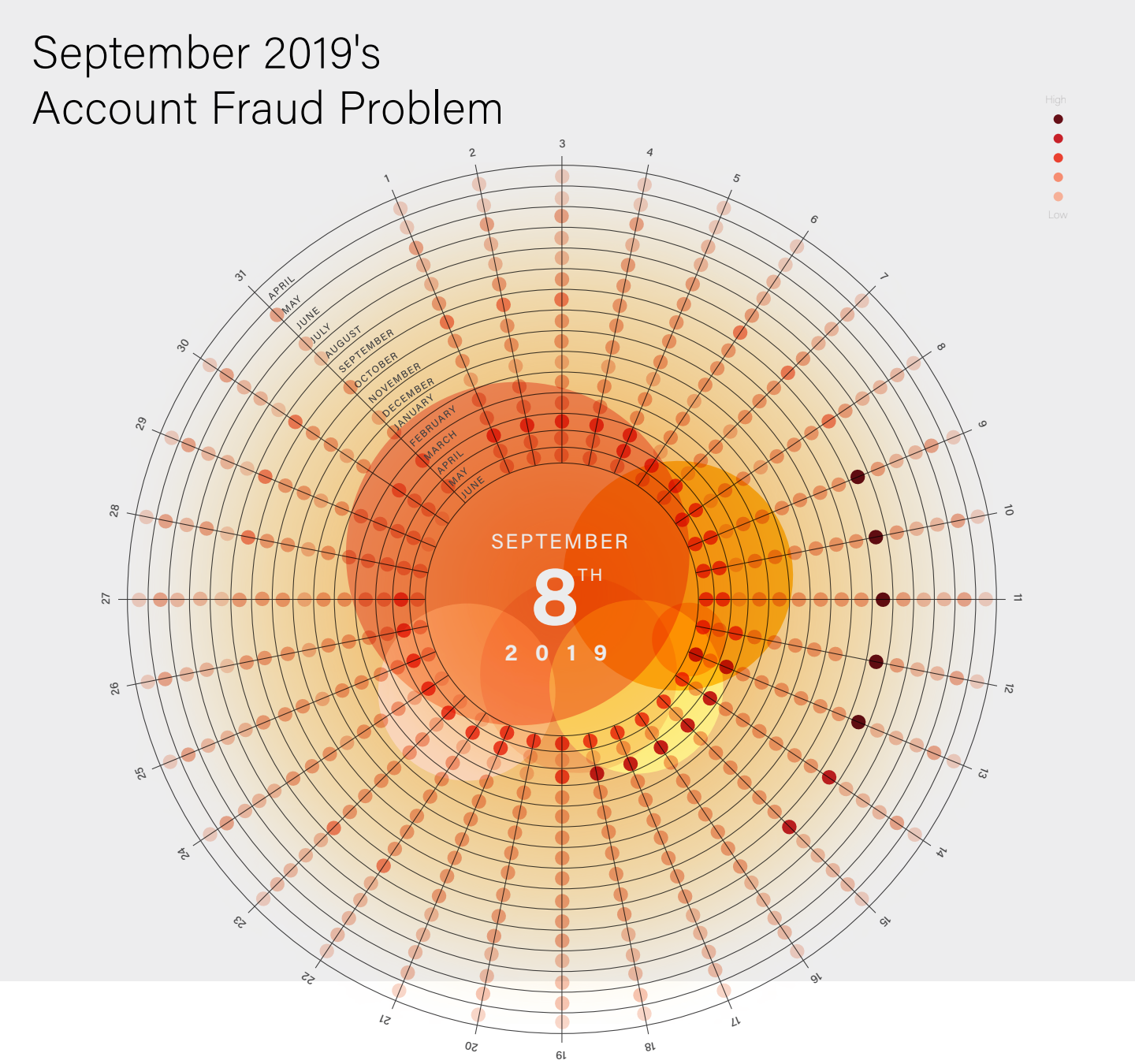
How and When ATO Fraudsters Attack

There's a common perception that cyber criminals are lone wolves; that the face behind the fraud belongs to one person with finite resources and too much time on their hands. But as illustrated by industry findings and Sift's network data, the scope, scale, and speed of digital fraud makes that perception impossible. The lonely, disgruntled hacker trope has mutated into far-reaching, state-sponsored teams of fraudsters who are just as focused on efficiency, expansion, and ROI as any e-commerce merchant.

Today's hackers are also planners. Their attacks are sophisticated and organized, timed for success, and focused on generating maximum returns. Between Q2 2019 and Q2 2020, ATO attacks happened in discrete waves about a week apart. September showed the highest spikes, with the highest number of ATO attacks taking place on the 8th.

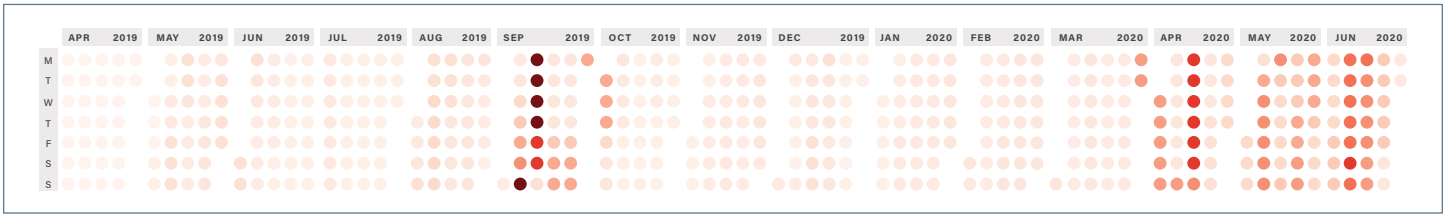
This dynamic attack pattern is a common, strategic numbers game in which fraudsters attempt to overwhelm fraud prevention systems and risk teams by hitting them with huge, widespread account takeover attacks. Even if the merchant has a fraud prevention solution in place, the hope is that a small percentage of those attacks will succeed, simply because there's too much fraud for it all to be blocked effectively.

Our data also illustrates that fraudsters are increasing their efforts during months that aren't usually considered the fraudiest time of year (the holidays). Instead, they're attempting to hide behind other predictable changes in traffic and transactions that take place year round. This is further supported by September 2019's account takeover data: flanked by two major, national e-commerce shopping seasons (back to school and the start of the holiday season), fraudsters saw and seized the opportunity to "hide" behind upticks in event volumes. Using the influx of traffic and transactions—and the possibility of risk teams bogged down by manual reviews—they'll attempt to more easily bypass security gates.



September 8, 2019: Fraudiest day of the year for individual account takeover attempts

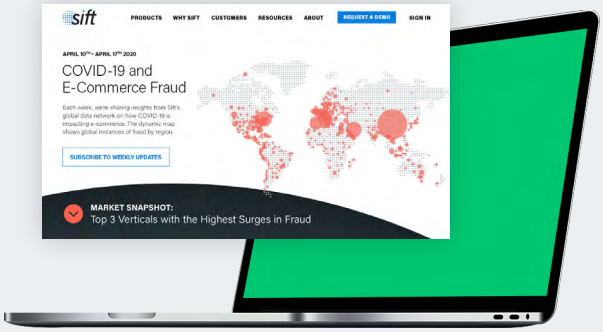
The above graph shows the number of attempted daily ATO attacks across the entire Sift network between Q2 2019 and Q2 2020. This period showed an interesting trend, as illustrated below: ATO attempts came in discrete waves, about a week at a time. Sift's Trust and Safety Architects suggest this was intentional and tactical. It's likely that fraudsters were attempting to overwhelm security systems in order to get past them (an especially successful approach if merchants don't have a dedicated ATO team or fraud solution).



Account Takeover is Changing Scope—Trust and Safety Teams Need a Real-Time Solution

The stakes are high when facing a threat that's as diverse, adaptable, and formidable as account takeover fraud. The only sustainable and scalable way to escape the constant back-and-forth between fraudsters and friction is to implement a solution that's seamless for trusted users and a barrier for fraudsters. With Sift Digital Trust & Safety, merchants can add friction points that fraudsters can't reverse engineer and that remain invisible to trusted customers, all while serving up the streamlined experiences they expect. Sift enables risk teams to stop fraud and fuel growth in real time, without insulting trusted users, and without spending countless hours on manual review.

Look out for our next Digital Trust & Safety Index to stay up to speed on how fraud is changing across e-commerce and how online merchants can keep customers secure while preserving revenue and driving explosive growth. You can also read our Q1 2020 report on the changing fraud landscape here, or get our Q2 2020 report on content abuse and the fraud economy here.



How COVID-19 Has Changed E-commerce

Since March of 2020, Sift has been tracking how fraud rates and event volumes are changing each week across multiple e-commerce verticals in response to the pandemic. This tracker represents a 7-day moving average to illustrate the acute effects COVID-19 is having on online merchants. In many cases, slowdowns in traffic are driving fraud rates higher because the average number of fraud attacks is being calculated against declining event volumes. But in some verticals, such as physical e-commerce, fraud has risen in tandem with surging traffic —an expected byproduct of more consumers turning to online shopping and services to reduce in-person contact while lockdowns continue, and fraudsters prey on the disruption. Explore detailed findings here.

About Sift

Sift is the leader in Digital Trust & Safety, empowering businesses of all sizes, from digital disruptors to Fortune 500 companies, to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of 35 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Twitter, Airbnb, and Twilio rely on Sift to gain competitive advantage in their markets. Visit us at sift.com and follow us on Twitter **@GetSift**.

Sources

1. *Comparitech, "Identity theft facts & statistics: 2019-2020." https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/*
2. *Global X, "A Decade of Change: How Tech Evolved in the 2010s and What's In Store for the 2020s." https://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and-whats-in-store-for-the-2020s/*
3. *Forbes, "What Constitutes A Restaurant In America Is Changing." https://www.forbes.com/sites/aliciakelso/2019/10/03/what-constitutes-a-restaurant-in-america-is-changing/*
4. *On behalf of Sift, Dynata polled 1,000 adults across the United States via online survey, age 18+, in August, 2020.*
5. *Fundera, "Ecommerce Shopping Cart Abandonment Statistics (2020)." https://www.fundera.com/resources/shopping-cart-abandonment-statistics*
6. *Digital Shadows, "From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover." https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover*
7. *Sift, "Digital Trust & Safety Index: Content Abuse and the Fraud Economy." https://resources.sift.com/ebook/digital-trust-safety-index-content-abuse-and-fraud-economy/*
8. *Dark Reading, "Password Reuse Abounds, New Survey Shows." https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689*
9. *TechJury, "How Much Time Do People Spend on Social Media in 2020?" https://techjury.net/blog/time-spent-on-social-media/*
10. *Norton, "Online Dating Scams and How to Protect Yourself." https://us.norton.com/internetsecurity-online-scams-online-dating-scam-statistics.html*
11. *Google, "Online Security Survey: Google/Harris Poll - February 2019." http://services.google.com/fh/files/blogs/google_security_infographic.pdf*
12. *Bank Info Security, "The Costs and Risks of Account Takeover." https://www.bankinfosecurity.com/blogs/enzoic-5-p-2768*
13. *Okta, "3 Common Mistakes That Lead to a Security Breach." https://www.okta.com/identity-101/mistakes-that-lead-to-security-breach/*
14. *TechCrunch, "Hacker who stole 620 million records strikes again, stealing 127 million more." https://techcrunch.com/2019/02/14/hacker-strikes-again/*
15. *PayPal, "Five e-commerce fraud trends to stay on top of right now." https://www.paypal.com/us/brc/article/2020-ecommerce-fraud-trends*
16. *Chargebacks911, "Chargeback Stats." https://chargebacks911.com/chargeback-stats/*
17. *Chargeback Gurus, What is Friendly Fraud? How can I prevent it? 2020." https://www.chargebackgurus.com/blog/friendly-fraud-its-a-family-affair*
18. *Chargeback, "2019 True Cost of Fraud Report." https://chargeback.com/2019-true-cost-of-fraud-report/*
19. *Sift, "COVID-19 Chargebacks: Where We Find Ourselves Now." https://resources.sift.com/webinar/covid-19-chargebacks/*
20. *Sift, "COVID-19 and E-commerce Fraud." https://sift.com/covid-19*
21. *F-Secure, "State Sponsored Cyber Attacks." https://www.f-secure.com/us-en/consulting/our-thinking/state-sponsored-cyber-attacks*
22. *Sift, "Digital Trust & Safety Assessment." https://pages.sift.com/digital-trust-and-safety-assessment-request.html*
23. *Sift, Digital Trust & Safety Index: A Rapidly-Changing Fraud Landscape." https://resources.sift.com/ebook/digital-trust-safety-index-a-rapidly-changing-fraud-landscape/*