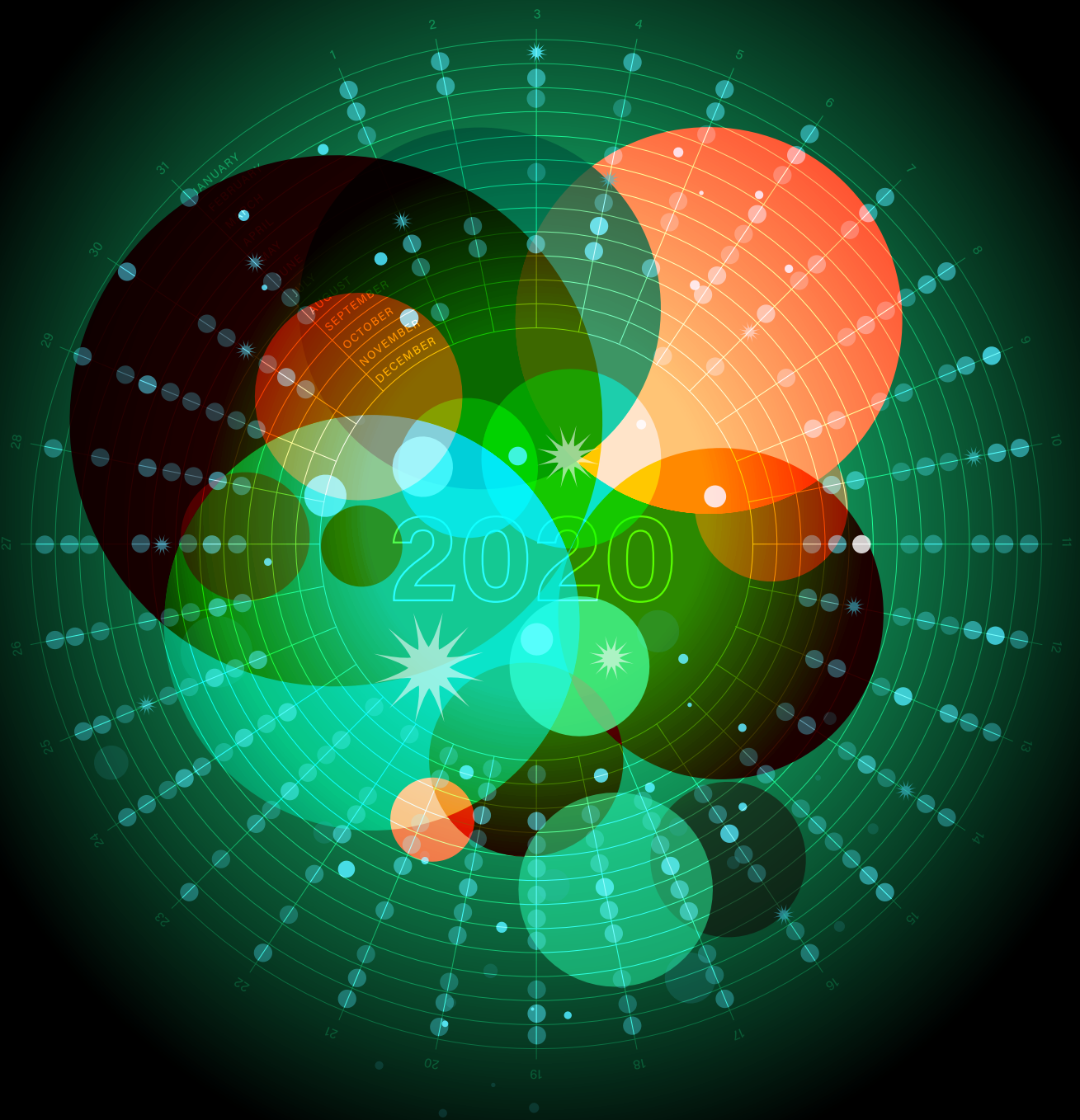
sift

Q4 2020 DIGITAL TRUST & SAFETY INDEX

Holiday Fraud and the Shifting State of E-commerce



Contents

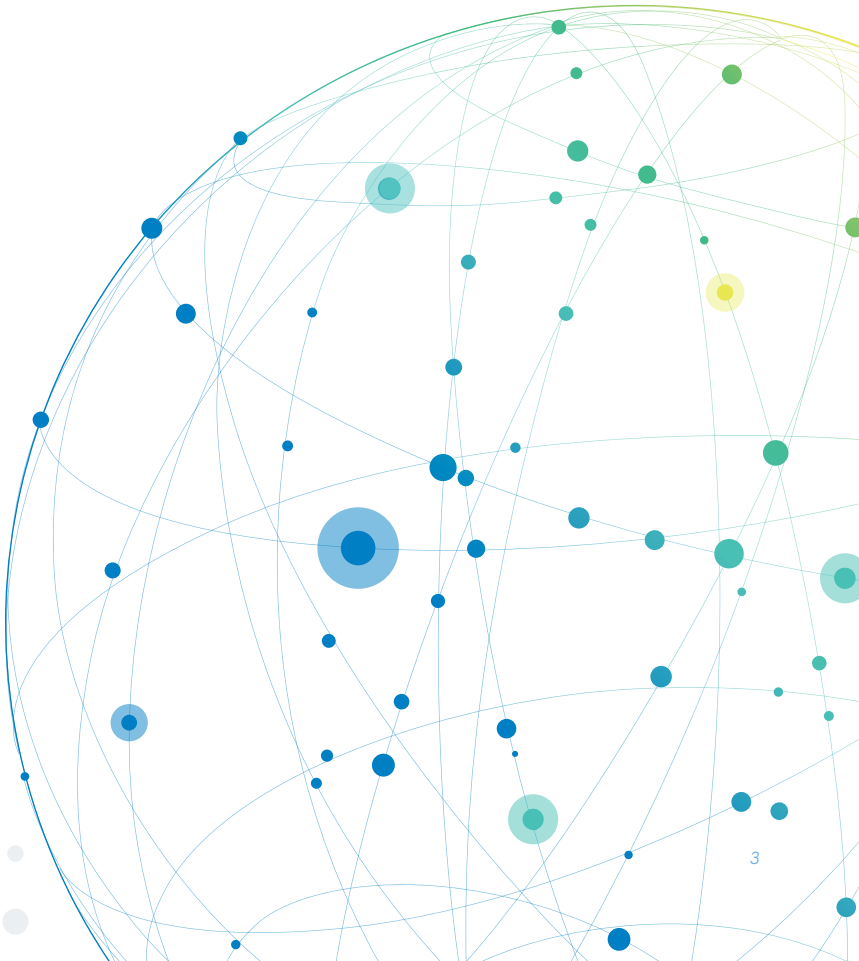
The Changing State of E-commerce Fraud

In January of this year, trust and safety experts predicted that 2020 would be a period of growth and innovation. They expected important, but iterative, developments in fraud prevention technology: bot protection, increased use of biometrics and behavioral analytics, and widespread adoption of MFA and 3DSecure. And while some of those predictions came true, no one managed to guess at the coming chaos that would turn e-commerce inside out and upside down over the coming months.

As COVID-19 continues to force merchants to lean into ballooning digital demand and no-contact shopping, fraudsters are seizing the chance to make their methods more targeted. They're opting for fewer, higher-value attacks spread across longer time periods, in lieu of rapidfire attacks that are worth less on average but happen more frequently. And as we wrap up an unforgettably challenging and volatile year, data indicates that the priority for trust and safety teams won't be to assess how *much* fraud there was during the pandemic. Instead, risk teams will need to focus on how intentional, strategic, and valuable fraud attacks have become because of the disruption COVID-19 has caused, and how months of erratic market shifts have exposed new loopholes and vulnerabilities for fraudsters to exploit.

The data in this report is derived from multiple consumer surveys* conducted throughout 2020, as well as Sift's global network of customers representing over 34,000 sites and apps. These findings have been interpreted by our team of data scientists and fraud analysts to give merchants insight into the fluctuating state of digital fraud, as well as illustrate how this year's disruption has forever changed the shape of e-commerce.

**On behalf of Sift, Dynata conducted two (2) polls of 1,000 adults (age 18+) per poll across the United States via online survey, in June and August of 2020.*



How Digital-First Holiday Shopping Changed the Game

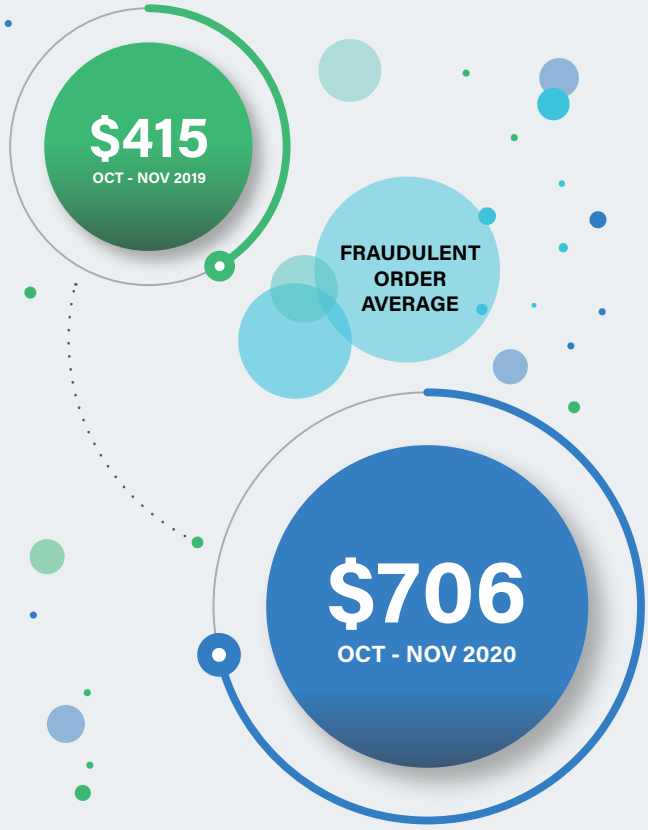
If 2020 is remembered by e-commerce professionals for one thing, it'll likely be the number of times they received an email with the word "unprecedented" in it. But despite the operational and demand changes businesses were forced to make, merchants and fraudsters alike saw a golden opportunity to profit off of increased transaction volumes—particularly during a digital-first holiday rush.

And profit they did: as much as an uptick in digitally-driven sales was to be expected, the holiday sales jump not only blew past expectations, it began long before temperatures dropped and seasonal decor went up. From April to November of 2020, the average daily order value per transaction was **9% higher** than the average daily order value per transaction during 2019's entire Black Friday weekend, a span of just three days. Also between April and November of 2020, e-commerce merchants have enjoyed Black Friday-like order volumes every day: average daily transaction volumes across the Sift network were equal to about **88% of the average daily transaction volume** that occurred during Black Friday weekend 2019.

Unfortunately, fraudsters got smarter and more intentional about their attacks during this time, too, relying on huge upswings in traffic and transactions to skirt past security measures. Food and beverage was hit hard—on November 29, 2020, **average attempted fraudulent purchases surged to over 475% of October and November's average**, as fraudsters looked to hide beneath the cover of restaurants' and delivery services' Black Friday Weekend deals. And, while Sift data shows that cybercriminals are launching fewer attacks at once and over extended periods of time, **each attempted fraudulent purchase across e-commerce is now worth an average of 70% more than they were last year**, increasing in value from $416.00 USD in October/November 2019 to $710.00 USD in October/November of 2020.

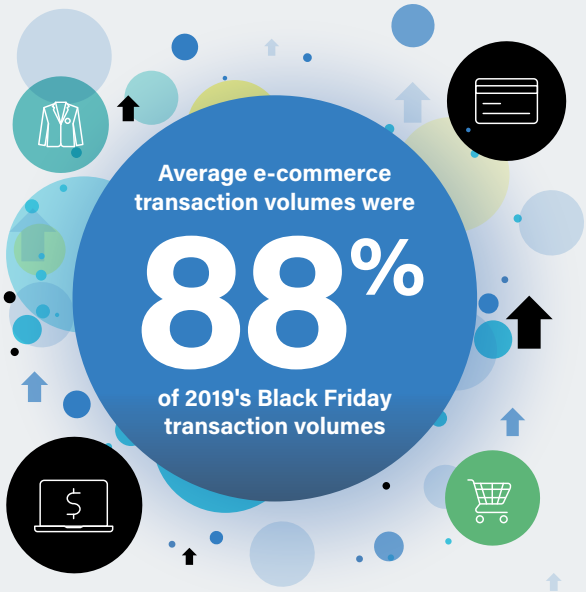
Fewer Attacks, Bigger Profits

Average fraudulent order values 2019 vs. 2020



There are a handful of reasons this is happening, not least of which is that merchants everywhere must consider where their customers' dollars are now being spent. Businesses don't want to insult trusted or first-time users who might just be avoiding brick-and-mortar stores. And, previous risk thresholds can't account for the onslaught of legitimate purchases now happening online—but raising those thresholds makes it easier for fraudsters to steal, and they know it.

Every Day is Now Black Friday: Surging Digital Demand April – November 2020



Since April of this year, average **daily** volumes are equal to **~88% of the transaction volume** that occurred during Black Friday weekend 2019, which took place between Friday, November 29th and Sunday, December 1st. The average daily order amount for April-November 2020 was also **9% higher** than the average daily order amount during 2019's entire Black Friday weekend.

Between March and August of this year, physical e-commerce saw a 378.26% jump in account takeover fraud, a byproduct of shifting opportunities to exploit these types of businesses. BOPIS (buy online, pickup in store) and BORIS (buy online, return in store) transactions have made shopping safer, but for merchants that choose to forgo 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.

With months, and perhaps years, left to face the echoing impact of COVID-19 on e-commerce, it's critical that trust and safety teams understand how the stakes have changed. The cost of every lost customer, every chargeback, and every fraudulent purchase is greater, and their damage more lasting. Risk teams can't treat this evolving fraud strategy as a seasonal anomaly—instead, this may just be the new normal that everyone's been talking about.

Fraudsters are masters of testing a company's security limits, and they put a lot of effort into identifying and exploiting the loopholes they find—but they're not reckless.

With the pandemic's impact, cybercriminals are taking bigger swings by increasing the value of their attacks and attacking more channels. But by spacing them out over time and turning down the volume on blitz-style abuse, fraudsters have become more difficult to pinpoint, and fraud much harder to prevent.

For merchants relying on rules-based fraud prevention and manual review that simply can't scale quickly enough to keep up with this shift, it's a worst-case scenario.

Kevin Lee
Trust and Safety Architect, Sift

The Widespread Reach of Online Fraud

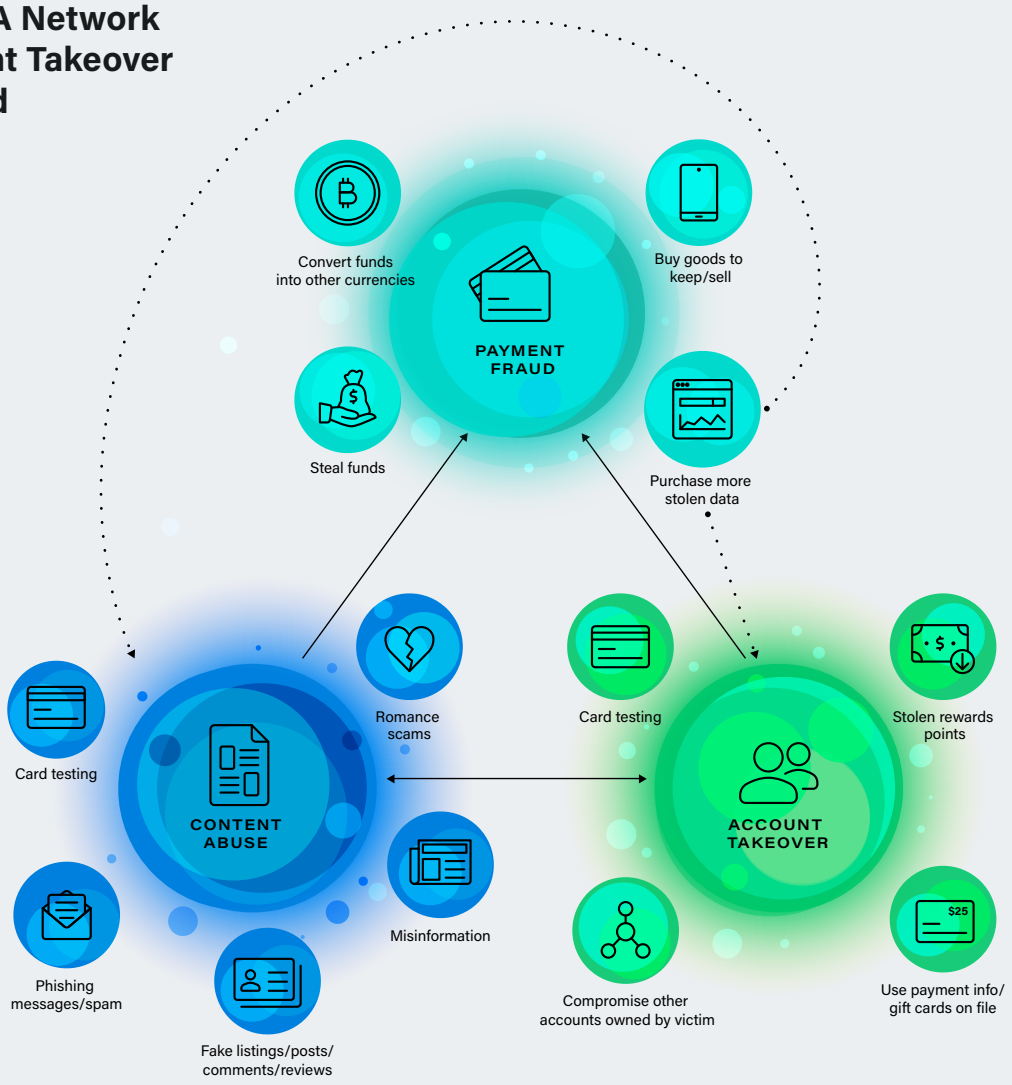
Fraud is nearly always a stepping stone used by cybercriminals for some type of financial gain. So, it's helpful to think of fraud vectors in the context of a supply chain, wherein each type of abuse is connected either directly or indirectly to payment fraud, and each vector can serve as a gateway to another.

The Fraud Supply Chain: A Network of Content Abuse, Account Takeover (ATO), and Payment Fraud

PAYMENT FRAUD is often the end goal, and content abuse and ATO can both serve as stepping stones towards stealing money. Funds can be used to buy goods to keep or resell, or to buy more data on the dark web.

ACCOUNT TAKEOVER (ATO) exposes payment, gift card, and rewards points details protected behind credentials. Stolen information is used to test cards, open accounts under the victim's name, post fake or malicious content via their networks, or—in the case of poor password hygiene—compromise other accounts the victim owns.

CONTENT ABUSE enables payment fraud and account takeover by convincing consumers to share credentials or send money via fake or malicious messages, phishing, misinformation, or romance scams.

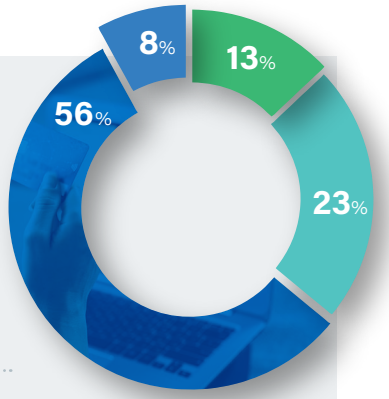


For e-commerce merchants, this interconnectivity between fraud vectors can compound the consequences of content abuse, account takeover, and payment fraud. Consumers have repeatedly reported that falling victim to an attack on an app or website would forever damage their relationship to the compromised brand.

Churn, Chargebacks, and Future Consequences

Over half of consumer respondents to a June 2020 survey by Sift said that, if they learned that their personal information had been exposed as a result of a malicious content scam on a website, **56% would stop using the site or service and choose a different provider.**

Spam, Scams, and Brand Abandonment



- **Stop using the site or service and select another provider: 56%**
- **Keep using the site/service, but change credentials/personal info: 23%**
- **Keep using the site/service/contact support: 13%**
- **No change in behavior: 8%**

The same is true for account takeover fraud, with **28% of consumers reporting that they'd leave a business behind** after having their account hacked or otherwise compromised via that brand's online properties.

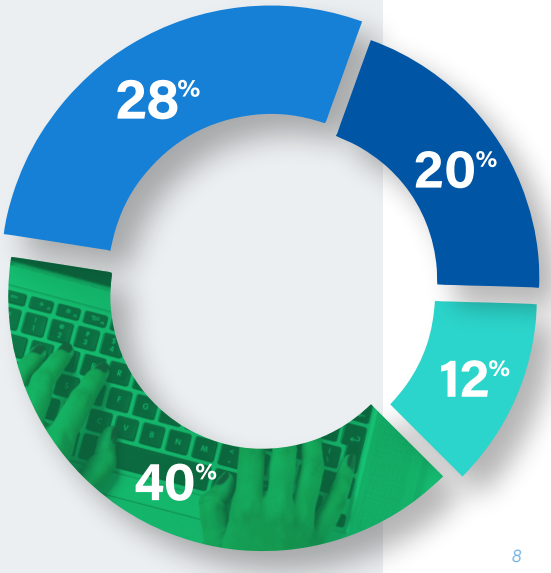
Preventing account takeover, in particular, is critical to preventing financial losses incurred from restoring customer balances after their accounts are hacked and money is taken. Securing customer accounts is also critical because ATO is directly linked to brand abandonment, as well as another expensive fraud fallout: chargebacks.

While brand abandonment can be loosely measured in terms of the lost value of the average customer's cart, the total damage done when customers churn can't be quantified. If lost sales are considered in the context of the average customer's lifetime value (LTV), as well as customer acquisition costs (CAC), the consequences get exponentially bigger—and most of those measurements don't include the impact of negative reviews.

Chargebacks can become even costlier than lost customers, leading to considerable financial loss, wasted time, and thinning resources. 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 account takeover. Once a customer discovers that an account they own has been hacked, they'll demand refunds, store credit, or replacement items—and the business will have to eat the cost.

ATO Costs Customers and Capital

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.**



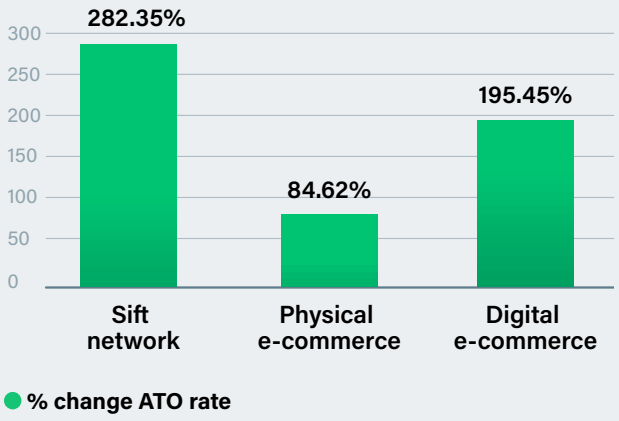
- **Keep using the site/service, but change credentials/personal info: 40%**
- **Stop using the site or service and select another provider: 28%**
- **Keep using the site/service, and contact support: 20%**
- **No change in behavior: 12%**

2020: Fraud Goes Mobile, ATO Takes Center Stage

Between Q2 of 2019 and Q2 2020, **account takeover fraud rates skyrocketed by 282%.** This massive increase represents the percentage of total logins across the entire Sift global network that were stopped because they were fraudulent; specific verticals, like physical and digital e-commerce, also saw fraud rates rise significantly.

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

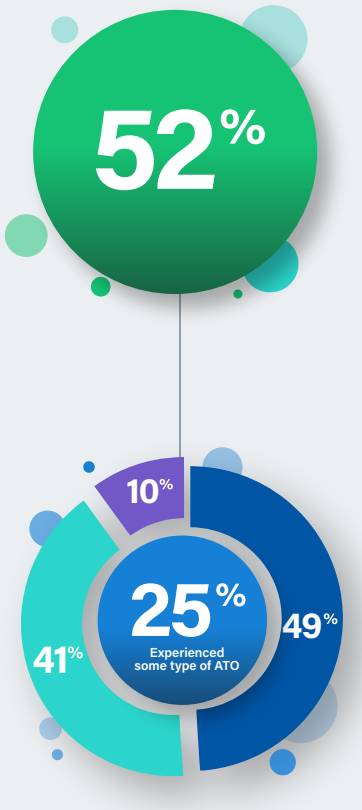
The below graph represents the percent change from Q2 2019 to Q2 2020 for overall ATO rates (the percentage of total logins that were stopped because they were fraudulent). Data is illustrated for the entire Sift network, and individually separated out for physical e-commerce and digital e-commerce.



Considering the potential damage of fraud to brand loyalty and a business's bottom line, it's critical that merchants know what they're actually up against. In addition to these clear upticks in attempted fraud, most victims—specifically of account takeover—report that they've been defrauded more than once, with nearly half of them **(41%)** facing ATO 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

One major contributing factor to this rising account fraud—and evolving fraud methods throughout e-commerce—has been the explosion of new digital payment options available between 2019-2020. Credit cards are no longer as vulnerable as they once were, and according to research from earlier this year, are no longer one of the most common payment types exploited by fraudsters. Instead, digital-only innovations account for three of the top five payment types most associated with fraud, a clear indicator that fraudsters are dedicated to taking advantage of emerging technologies in order to diversify not just where, but *how* they steal from businesses and consumers.

Sift also found that the average fraudulent purchase attempt was **about three times the amount of a legitimate transaction**—an issue exacerbated by the changes merchants have been forced to make in pandemic-era e-commerce, such as relaxing risk mitigation strategies and fraud thresholds to account for a year of unprecedented online shopping.

The majority of fraudsters have left their proverbial basements, too, and aren't executing attacks via laptops or desktop computers. Instead, more than half (51%) of the payment fraud attempted between Q1 2019 and Q1 2020 was done via mobile devices. And during a year of no-contact shopping and new dependence on delivery services, those numbers have likely risen.

New Ways to Pay Mean New Ways to Steal

Cybercriminals have been flocking to exploit emerging forms of CNP and other online payment options. The following payment types, in order, were most associated with fraudulent transactions in 2019—and experts expect these trends to continue.

01 Online Promos

02 Digital Wallets

03 Money Orders

04 Cash

05 Cryptocurrency

06 Gift Cards

07 Credit Cards

08 In-App Purchases

09 Other Third-Party Processors

10 Rewards Points

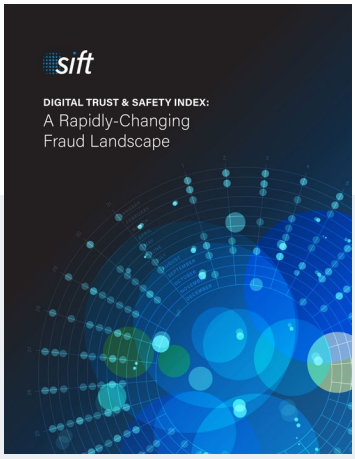
Readying Digital Trust & Safety in 2021

Fraud is damaging to all areas of business, and trust and safety teams already have to adapt how they fight it as vectors and risks change. The threat to companies and their customers is ongoing, making the need for comprehensive, adaptable, real-time protection a necessity for growth without risk.

The findings in this report reflect a year of disruption—but one of discovery, too. It's clear that fraudsters are nearly as innovative, flexible, and sophisticated in their attacks as the teams tasked with stopping them. Merchants need to consider the entire ecosystem of abuse to successfully address vulnerabilities throughout the customer journey, as well as across apps and websites.

Erratic consumer behavior and fluctuating market conditions will be a challenge for several more months, and many e-commerce businesses will feel the impact of 2020 for years to come. Implementing a Digital Trust & Safety approach enables business leaders to shape their entire strategy around growth and unmatched protection from all types of fraud—including emerging and evolving threats that are as unprecedented and unpredictable as this year has turned out to be.

Dig deeper into Sift's 2020 fraud data with each of our current Digital Trust & Safety Index reports:



A Rapidly-Changing Fraud Landscape

Payment fraud

Content Abuse and the Fraud Economy

Spam, scams, and content fraud

Account Takeover Fraud and the Growing Burden on Business

Account takeover and abuse

About Sift

Sift is the leader in Digital Trust & Safety, empowering 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. *Sift, "The Good, the Bad, and the Ugly: What Will 2019 Bring for Fraud?" https://blog.sift.com/2019/the-good-the-bad-and-the-ugly-what-will-2019-bring-for-fraud/*
2. *Visual Capitalist, "Investing in the Impending E-commerce Future." https://www.visualcapitalist.com/investing-in-the-impending-e-commerce-future/*
3. *Sift, "Q3 2020 Digital Trust & Safety Index: Account Takeover Fraud and the Growing Burden on Business." https://resources.sift.com/ebook/digital-trust-safety-index-account-takeover-fraud-burden-business/*
4. *Digital Commerce 360 Retail, "Tips to Fight Fraud During Covid Times." https://resources.sift.com/ebook/digital-commerce-360-retail-tips-to-fight-fraud-during-covid-times/*
5. *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/*
6. *Chargeback Gurus, "What is Friendly Fraud? How can I prevent it? 2020." https://www.chargebackgurus.com/blog/friendly-fraud-its-a-family-affair*
7. *Chargeback, "2019 True Cost of Fraud Report." https://chargeback.com/2019-true-cost-of-fraud-report/*
8. *Sift, "Digital Trust & Safety Index: A Rapidly-Changing Fraud Landscape." https://resources.sift.com/ebook/digital-trust-safety-index-a-rapidly-changing-fraud-landscape/*