



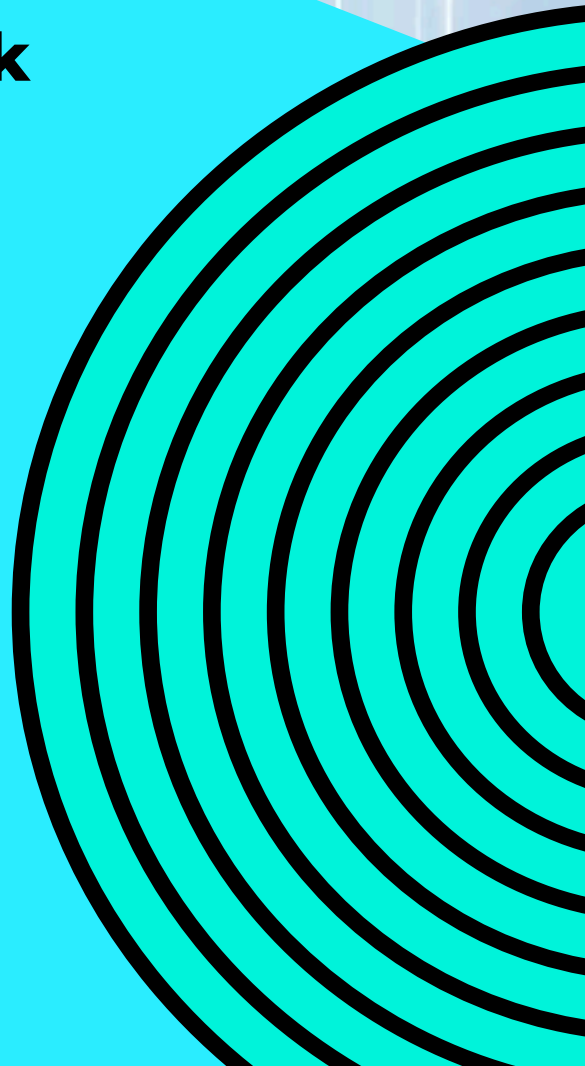
Merchant  
Fraud  
Journal



# 3 Ways a Unified Chargeback Management and Fraud Platform Increases Revenue



Sponsored by Sift



# Table of Contents

---

2 A unified platform detects risk signals at all potential points of failure

---

3 Integrating processes and data makes it easier to detect and prevent account takeover fraud (ATO)

---

4 Automation scales with you and improves your customer experience

---

7 About MFJ

---

8 About Sift

## 3 Ways a Unified Chargeback Management and Fraud Platform Increases Revenue

The Fraud Economy thrives because fraudsters consistently find vulnerabilities in merchants' defenses. For multi-channel retailers, the need to build payment ecosystems that ensure seamless customer experiences while minimizing chargebacks presents special challenges.

As an example, US Click-and-Collect sales more than doubled from \$35 billion to \$72.5 billion in from 2019 to 2020 ([link](#)). At the same time, multi-channel merchants used to have 1–2 days between an online order date and shipping from the warehouse; today, that number can be as low as 1 hour. That puts a lot more pressure to ensure orders are legitimate in a very short window of time.

Shorter review windows is just one example of new problems. New methodologies like content fraud—where cybercriminals infiltrate user-generated content channels (UGC) to run scams—have created entire new attack vectors to defend against.

As the pandemic recedes to a new normal, merchants must adapt to the new realities. Old ways of thinking in terms of siloed strategic objectives—chargeback prevention over here, customer experience over there—are not enough to stop the new fraud patterns that have emerged and continue to emerge.

Over one-third of retailers (34%) consider fraud and dispute management a high priority. In this report, we'll discuss three important ways integrating automated chargeback management into a single fraud and dispute management platform can increase revenue by preventing omni-channel fraud, protecting against the Fraud Economy, and safeguarding the customer experience at scale.

### A unified platform detects risk signals at all potential points of failure

New research shows that BOPIS (buy online, pick up in store) transactions increased 70% in volume in 2020 alone. ([link](#)) This is an overall trend that will continue to spike upwards overtime. The blend of online and brick-and-mortar risk signals presented new challenges for merchants.

Two categories of merchants developed: Those who shared traditional risk signal data collected in physical channels with digital channel fraud prevention models, and those who did not. Merchants taking the former approach have been much more successful at preventing fraud.

For example, merchants with BOPIS experience can cross-check in-store ID verification with online checks for high velocity purchases. This alerts fraud teams when a single person makes multiple purchases at multiple stores in a short timeframe—a strong fraud signal individual store checks alone cannot detect.

Building a single data lake for BOPIS orders affords merchants a large number of data-points to detect risk signals:

- Velocity of Use and Velocity of Change checks around the pickup person's name across all physical store locations (when the name is consistently validated by presenting Government issued ID)
- Negative list for pickup person's name (assuming ID check at pickup event)
- Recognizing when IP or mobile geolocation is in very close proximity to the pickup store location
- Quantifying distances between billing address, IP geolocation and pickup location
- Maintaining negative lists and velocity counts on name of person physically returning items purchased online
- Performing post-transaction analysis to identify online orders associated with high number of returns in-store
- Considering the duration of time between the online order date and the time of an in-store return
- Ensuring the order or transaction ID associated with an in-store return has not already resulted in a chargeback

Moving forward, merchants will need to detect these (and other) risk signals at all potential points of failure, pooling their systems' collective knowledge to build and adapt fraud models in real-time. A unified platform reduces inter-organizational barriers to collaboration by eliminating silos in favor of a company-wide approach. It also has no impact on the customer experience. Infact, the efficiency of a single platform can decrease approval times, reducing friction.

The average order value of a chargeback was \$241.99 in 2020, according to Sift Data Scientists. Successfully detecting risk signals at all potential points of failure will allow omni-channel retailers to avoid them while also increasing revenue through improved customer experiences, lower fraud rates, and increased their ability to dispute chargebacks that do occur.

## Integrating processes and data makes it easier to detect and prevent account takeover fraud (ATO)

The sudden acceleration of digital commerce over the last few years has opened up new opportunities for fraudsters. Account takeover (ATO) is one of the most popular ways fraudsters exploit vulnerabilities. Because ATO is a financial crime, merchants conceptualize it as a 'downstream' problem and deal with it only when payment issues appear.

Consumers do not view ATO this way. Theft of login credentials, banking information, or other personal information can create a cascade of knock-on problems. Merchants identified as the source of a breach that results in ATO attacks on customers instantly lose credibility and trust—74% of consumers would stop engaging if their account was hacked on a specific site or app.

Merchants must understand that consumers view information theft as the real crime; the downstream financial consequences just bring it to their attention. Preventing theft at checkout is not enough. Worse, many consumers reuse or rotate passwords across accounts, and 56% say that they store their personal and payment details with various online sites and apps. Consumers' demands for convenience compel merchants to accept responsibility for data they don't know how to adequately protect.

Fraudsters smell opportunity, deploying sophisticated "Proxy Phantom" tactics to attack merchants at scale. One sophisticated Proxy Phantom attack used bots and proxy servers to cycle through millions of usernames and passwords, all while hiding the attacks' origins by switching IP addresses in order to avoid getting blocked by typical rules-based fraud prevention systems.

It's little wonder then that there was a 307% increase in ATO fraud between April 2019 and June 2021, accounting for 39% of all blocked fraud across Sift's network in Q2 of 2021.

Together, these trends present huge challenges to merchants. Trust and safety teams must meet them by ensuring they don't idly allow customers' accounts to become testing grounds for fraud. This means detecting ATO risk signals prior to payment abuse, unauthorized transactions, or similar activities.

Failure to do so can result in significant revenue loss, churn, and disputes.

## Automation scales with you and improves your customer experience

New research shows that 92% of retailers believe a good dispute-management process can have a positive effect on customer satisfaction. Unified dispute management systems actively contribute to meeting this goal by creating positive data-feedback loops for all transactions in the retailer's payments ecosystem. As the data set deepens over time, so does its ability to effectively manage fraud and dispute processes.

Retailers must onboard technologies that can automate operations and fulfillment in order to apply the data set at scale. Fulfillment and dispute processes must meet the dual-goal of protecting retailers from chargeback fraud, without harming the digital experience. Legitimate customers increasingly demand seamless payment experiences, and any friction that interrupts the purchase process drives them into the arms of competitors.

Automating as much of the purchase process as possible allows it to be guided by data, which avoids common friction points such as incorrectly flagging orders for fraud or requiring overly-long manual review processes. Mistakes in the purchase process that can be traced back to missing or incomplete data do significant harm to revenue.

In addition, unified dispute management platforms bring new tools to the table such as Real-time Resolution, which allows retailers to communicate with a potential customer's issuing bank, resolving discrepancies before a dispute is even submitted.

***“If everyone is moving forward  
together, success takes care of itself”***

---

**Henry Ford**



# About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.





# About Sift

Sift is the leader in Digital Trust & Safety, empowering 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 Sift's unrivaled global data network of 70 billion events per month. Global brands including Airbnb, DoorDash, HelloFresh, and Twilio rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at [sift.com](https://sift.com), or follow us on LinkedIn.



### Contact Merchant Fraud Journal


Editor In Chief - Bradley Chalupski  
Bradley@merchantfraudjournal.com

---

### Contact Sift


www.sift.com  
sales@sift.com




 290 Caldari Road,  
Concord, Ontario L4K 4J4  
Canada

--

 hello@merchantfraudjournal.com

 www.merchantfraudjournal.com

 1-(888) 225-2909