# Fraud Prevention During Economic Unrest

Businesses of all types are scrambling to adapt to sudden shifts in both consumer behavior and fraud trends caused by the COVID-19 pandemic. Fraudsters are discovering more opportunities than ever to hide behind unexpected upticks or declines in order volume and exploit community unrest, forcing businesses of all sizes to adapt to these unprecedented circumstances.

## Protecting growth, preserving trust

To help fraud fighters understand what to expect in the coming months, and to keep their businesses and consumers safe from fraud as the situation evolves, Sift's team of Trust and Safety Architects (TASAs) have advice teams can implement quickly to adapt to fraud's new normal.

### Adjust policies and thresholds to accommodate new behavior

Consumer behavior has dramatically changed in the wake of COVID-19. People are stocking up on supplies, making higher-volume purchases, and exhibiting behavior that would have previously been deemed suspicious. Consider temporarily adjusting thresholds or sending more transactions to manual review. Doing so will keep false positives to a minimum while continuing to protect your business and its customers.

### Beware of BOPIS vulnerabilities

Consumers are turning to shopping options that involve less human contact, e.g., "buy online, pick up in-store" (BOPIS). This opens the door for fraudsters who will no longer face friction points like providing identification or a signature. Additionally, there may be a surge in account takeover (ATO) as credentials and credit cards are hijacked to place orders for in-store pickup, with fraudsters adding their own email addresses or names to account information to bolster the appearance of legitimacy. Consider adding more scrutiny to BOPIS orders.

### Prepare for more chargebacks and false positives

Merchants will likely see an uptick in chargebacks, as consumers and businesses alike face sudden, unexpected financial restrictions. Combine that with erratic buying behavior and a lack of historical data to inform whether or not transactions are legitimate, and trusted customers are likely to get declined—causing false-positive rates to rise. Still, the TASAs suggest looking at previous seasonality and year-over-year patterns for clues and cues on how to mitigate risk, and keep the context of the situation top-of-mind.

 | 

sales@sift.com

## Rely on experienced analysts, but don't overwhelm them

The TASAs suggest leaning more heavily on senior team members to make fraud decisions when presented with unprecedented situations. This comes with its own challenges—new remote-working environments, decision fatigue, overwhelming volume for certain industries—but the benefits could outweigh the cost. Trust and Safety leaders should consider redistributing work to better support overwhelmed analysts.

## Watch out for coronavirus-related scams and spam

Scams and spam content are always present online, but what's different right now is that fraudsters have fear and uncertainty about the pandemic to capitalize on. Beyond the financial and emotional harm fraudulent content can cause, people will lose trust in the businesses connected with it. Consider using machine learning to stop spam content affecting your business; when you can train models off of all of the signals on your site, and understand *how* content is posted (in addition to *what* is posted), you will have a better chance of getting ahead of spam.

## Communication is crucial during uncertain times

In the face of a global pandemic, communication, both internally and externally, is required to ease fear and set expectations. Internally, communicate the changes being seen throughout the business each day—between company leaders and fraud prevention teams, as well as throughout the larger workforce, for a 360° view into any impact the pandemic is having on the organization. Externally, use support centers, FAQs, emails, and in-app messaging to let your customers know the steps you are taking, and if they will experience things like shipping delays or limited inventory.

## Digital Trust & Safety with Sift | Together with our partners, we are building a safer internet

Sift is the leader in Digital Trust & Safety. Powered by the most sophisticated, real-time machine learning technology and a global community of fraud fighters, we combine custom models with learnings from across our global network of 34,000 sites to identify trusted users and fraudsters with unparalleled accuracy. Sift detects evolving fraud patterns automatically—enabling you to reduce losses and build trust with customers without the need to scale manual review efforts when user and transaction volumes grow.

**Partner with Sift to manage this period of uncertainty and protect your company's growth.**
Reach out to sales@sift.com for a Digital Trust & Safety assessment.