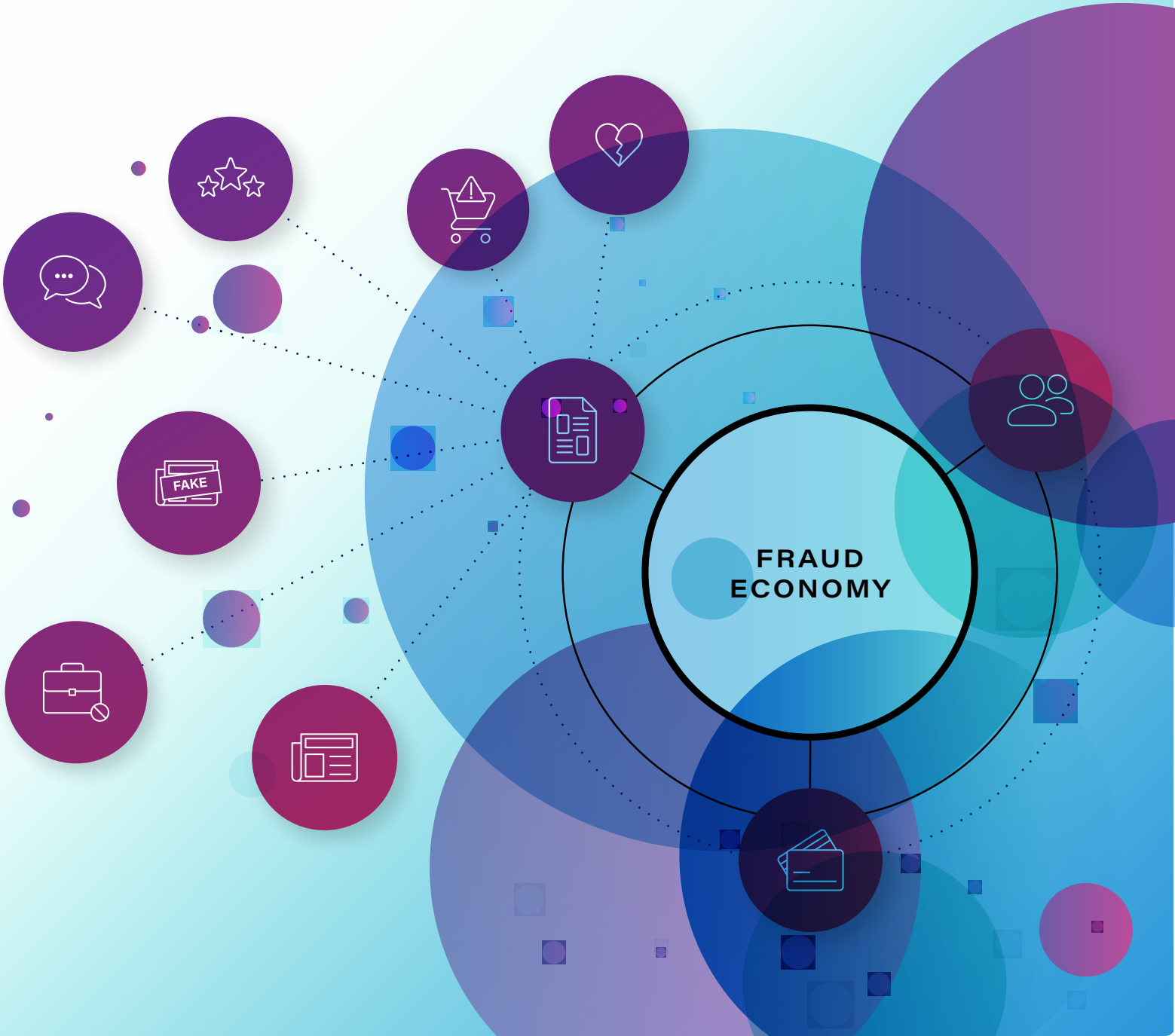
sift

Q2 2021 DIGITAL TRUST & SAFETY INDEX

How Spam and Scams Mobilize the Fraud Economy

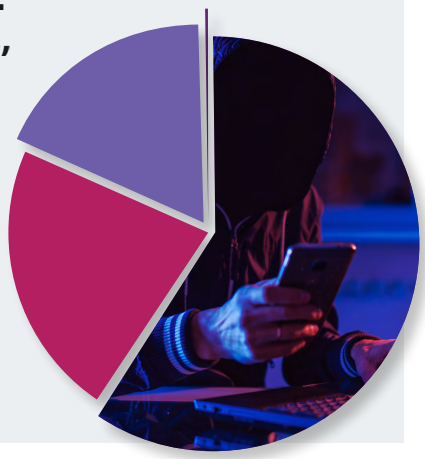


Contents

The Fraud Economy's Big Scam

Scams are the foundation of the Fraud Economy. This global, interconnected network of online abuse is motivated by the outcomes of conning consumers—and digital content is a ready-made disguise for fake information, financial fraud, and phishing. In fact, during the first quarter of 2021, scams made up nearly **60% of the abusive content blocked by Sift**.

Fraud Encounters: Phishing attempts, scams, and spam

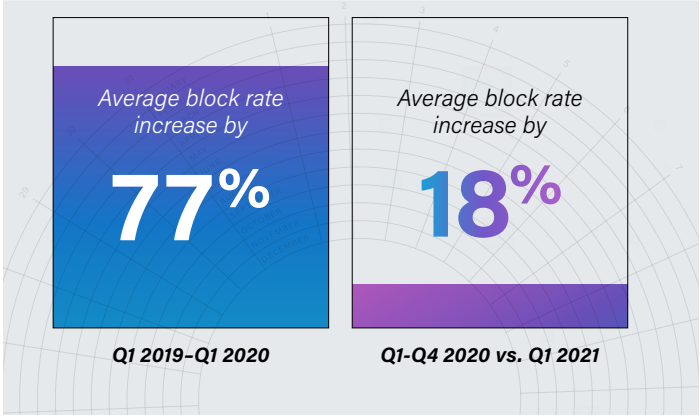


Scams	**59.4%**
Irrelevant	22.2%
Toxic	18.3%
Commercial	1%

*See footnote

Content fraud—when cybercriminals leverage user-generated content (UGC) to disseminate scams and spam on trusted websites, and trick consumers into sharing sensitive information—is especially difficult to detect before it's done harm. Forums, marketplaces, social media channels, and other websites often invite users to post and communicate independently from the business and without much oversight, making fake or suspicious messages hard to track even after they're identified, and inspiring a growing number of fraudsters to leverage malicious content for profit. The average rate of fraudulent content blocked by Sift spiked dramatically between Q1 2019 and Q1 2020, increasing by **77%**. And in just the first quarter of 2021, that block rate jumped another **18%.**

2019-2021: Rising content fraud year-over-year



Unexpected consumer behavior and disruption to business-as-usual were hallmarks of e-commerce throughout the pandemic. Market fluctuations created vulerabilities that many businesses had never faced, but that fraudsters were quick to exploit. As the world reopens, cybercriminals are adapting their methods faster than companies can adopt defenses—and the fraud patterns that emerge throughout 2021 will forecast the shape of things to come in a post-pandemic market.

The findings in this report are derived from Sift's global data network representing over 34,000 sites and apps using Sift, as well as responses from 1,200+ consumers surveyed in May 2021.** This data illustrates how content-driven attacks move the Fraud Economy forward, highlighting why and how fraudsters weaponize digital content.

*For detailed descriptions of fraudulent content types, see Sift's public documentation.

**On behalf of Sift, Researchscape International polled 1,265 adults (aged 18+) across the United States via online survey in May 2021.

2021 Emerging Industry Trends & Consumer Insights

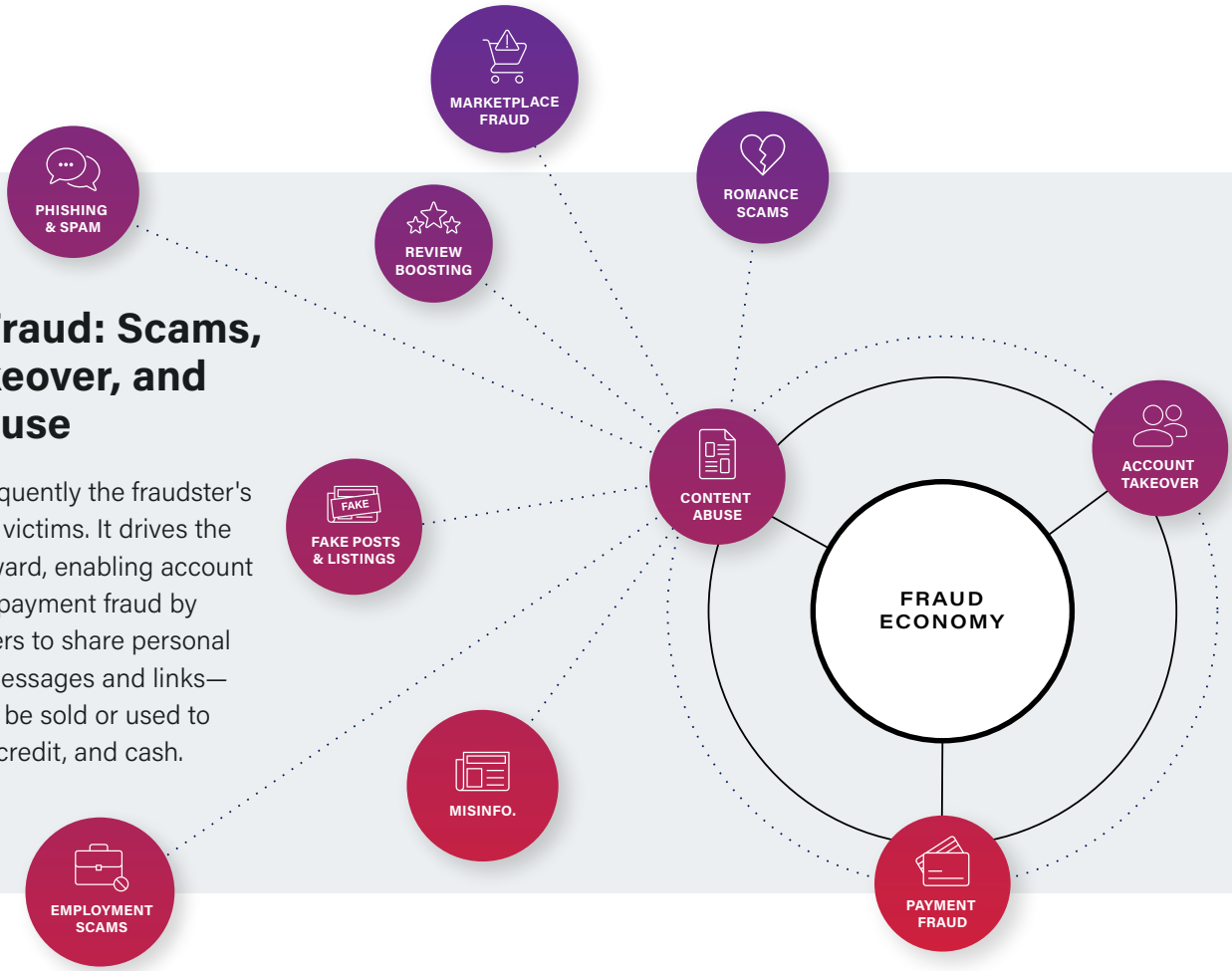
Last year's 77% increase in blocked content fraud from 2019 was a detrimental combination of rising attacks coupled with dwindling transaction volumes in multiple markets. But the current overall rate for 2021 is already trending upward from that spike. Incident rates have yet to dip back down to pre-pandemic levels, demonstrating that content-based attacks are just as prolific as they were when the COVID-19 pandemic first hit, if not more so, despite traffic and transaction volumes rising quickly as businesses bounce back this summer.

Recent industry reports state that BOPIS (buy online, pick up in store) transactions increased **70%** in volume last year, leaving merchants scrambling to protect new commerce channels from a type of fraud they'd never seen before. The sudden, rapid expansion to digital shopping and services, contactless delivery, social media shopping experiences, and hybrid retail experiences like BOPIS/BORIS (buy online, pickup/return in store) appears to have made consumers more wary of who they're really dealing with online. New research found that trust in a brand is the primary driving factor behind where people choose to spend their money.

Consumers' growing caution is warranted: as illustrated previously, scams made up well over half of the content fraud blocked by Sift in Q1 2021, and **~27% of surveyed consumers** report that they run across fraudulent content on a daily or weekly basis.

Symbiotic Fraud: Scams, account takeover, and payment abuse

Content abuse is frequently the fraudster's first touch with their victims. It drives the Fraud Economy forward, enabling account takeover (ATO) and payment fraud by convincing consumers to share personal data via malicious messages and links—information that can be sold or used to steal rewards, store credit, and cash.



Similarly, half of consumers surveyed say spam **(51%)** and scams **(50%)** are the types of fraudulent content they encounter most frequently, with misinformation and "fake news" **(43%)** following closely behind. But many companies are only equipped to react to fraud once they've been notified by users—users that businesses often rely on as their sole way of identifying suspicious messages and spam cropping up on their sites.

Merchants that depend on users to flag risky content aren't just leaving the doors wide open for fraudsters. They're actively contributing to their own financial losses—**more than half of consumers would stop shopping at a business and leave for a competing merchant** if they discovered malicious content on a brand's website. Additionally, bad actors will continue exploiting vulnerabilities against a platform until the merchant takes a more proactive stance at detecting fraud.

Consumers Prioritize Trust Over Trademarks

56%

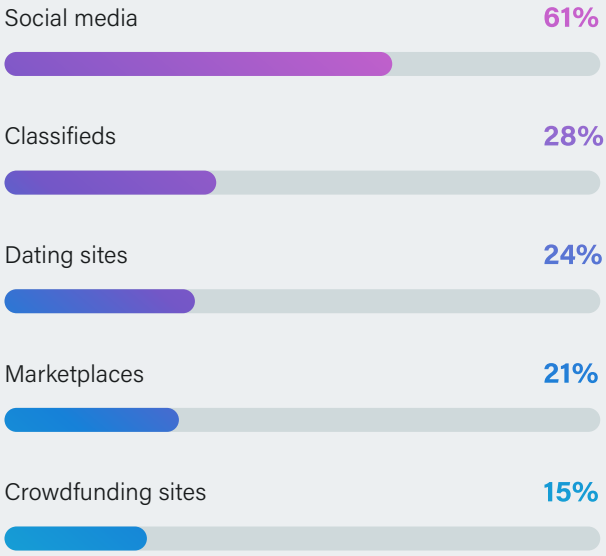
Stop using the site or service if they encounter fake/misleading content

54%

Stop using the site or service if they were successfully scammed into sharing personal info

Over one-third of consumers **(34%)** might still come around, but say they'd visit a scam-tainted site much less frequently. To put that in perspective: a single, successful scam on a merchant site could cost the potential profits of any immediate lost sales combined with those spurned shoppers' CAC (customer acquisition costs), LTV (lifetime value), and chargebacks resulting from any payment fraud that occurs using information exposed by the scam.

Survey Says: Consumers flag the top 5 spammiest and scammiest places online



Consumers report running into fraudulent content most frequently while visiting social media sites and classifieds—places the public has long known are breeding grounds for scams and fake information. Even with consumers' growing awareness online, merchants running ads on these platforms run the risk of copycat fraudsters mimicking their content to obscure malicious links or steal payment details from unsuspecting shoppers.

But those tactics are old news, and COVID-19 granted fraudsters myriad opportunities to exploit more sophisticated fraud systems and strategies. During pandemic lockdowns, entertainment and travel merchants saw transaction volumes fall to historically low levels. But dating sites, marketplaces, and fundraising platforms slid squarely into fraudsters' crosshairs, and the repercussions—rising chargebacks, higher rates of account takeover, compromised user forums, and further dissemination of malicious content—are still unfolding today.

DECONSTRUCTING CONTENT FRAUD:

Strategies and Methods

In a recent interview with Sift, ex-fraudster and risk expert Alexander Hall stated that "COVID-19 presented the perfect storm for fraud, leading e-commerce merchants to shift in ways that, unfortunately, fuel more sophisticated and widespread online fraud attacks."

Many businesses, seemingly overnight, pivoted as best they could and went digital in response to the crisis. They implemented contactless delivery, processed BOPIS/BORIS and telephone orders, and began allowing alternative digital payments.

While consumers quickly warmed to the newfound conveniences, fraudsters, expectedly, exploited them, using content fraud as a vehicle for theft. Promo abuse impacted businesses using discounts to stay afloat. Cybercriminals targeted fundraising platforms, and very early on, used fake content to push counterfeit vaccines or alternative "cures" for COVID, all of which were designed to steal cash from unsuspecting, vulnerable consumers.

For the foreseeable future, merchants will sit in the thick of this exploitation. Trust and safety teams need to be aware of how the evolving Fraud Economy will continue impacting pandemic-era market changes that are here to stay. And to do that, they'll need to think like the fraudsters that run it.

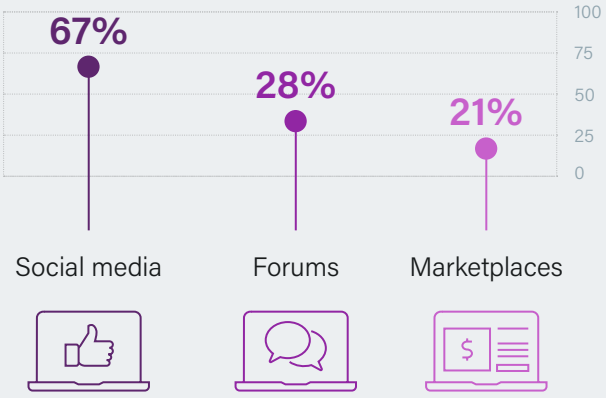
Hall's breakdown of a successful content scam, based on his personal experiences as a fraudster, focuses on the exploitation of existing systems to commit fraud, and sheds light onto that criminal thought process. His fraud operation followed an established but profitable playbook: diversify targeted channels, delegate responsibilities across multiple players (up to 150 in Hall's case), forge digital and physical documents using legitimate paperwork, and most critically, always work as much as possible within the parameters of a company's existing security systems and checkpoints.

In other words, don't break the rules—work around them. He warns that fraudsters are using these same tactics now to take advantage of COVID-inspired operational changes: studying a business and seizing natural opportunities to defraud and avoid friction, rather than attempting to hack a merchant website behind the scenes.

It's All a Scam: Fraudsters and fakers exploit COVID-19

50% of consumers believe they have encountered COVID-19 scams or misinformation

Where pandemic-related misinformation was found



Top misinformation claims

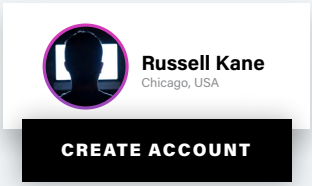
The vaccines are ineffective against COVID-19 or induce other diseases or ailments **61%**

The vaccines contain technology that allows people or governments to track those who get the vaccine **61%**

Fraudulent vaccine cards/passports **28%**

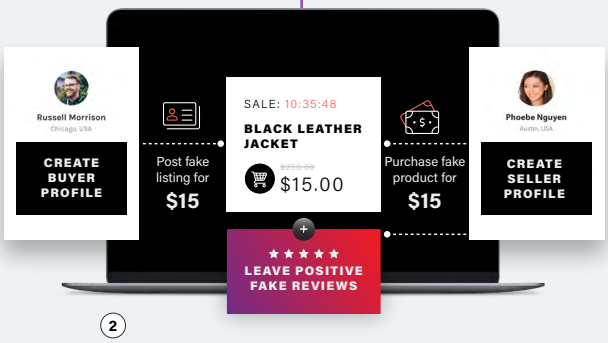
How it Works: Mechanics of a marketplace scam

Marketplaces are top targets for scam artists, allowing fraudsters to manipulate both buyer and seller accounts to maximize profits. In many cases, cybercriminals deploy scammy content as the first step of a larger payment fraud operation—sometimes webbing off from just one fake listing to create a chain of phony posts, or use stolen data across the marketplace.



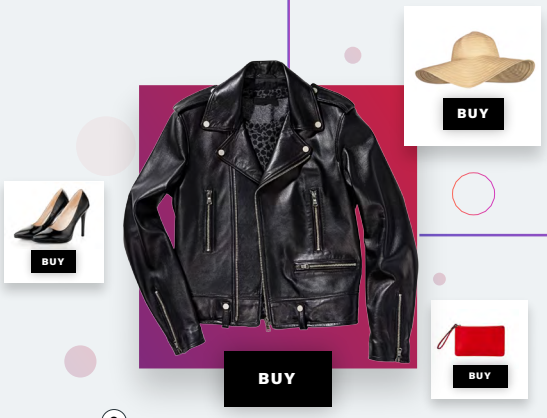
1

Set up shop on a marketplace with fake or stolen card information, creating a seemingly legitimate reputation by leaving positive fake reviews.



2

Test hijacked credit card and (if applicable) gift card information.

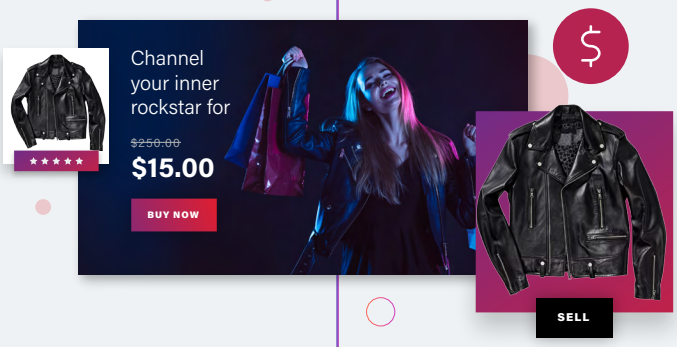


3

Use viable card information to purchase more goods on the same marketplace or other websites.

4

One scam, limitless damage
Resell ill-gotten goods to unsuspecting customers, allowing fraudsters to profit in a multitude of ways:



Profit + data
Send the goods, pocket the profit, and keep or sell the victim's personal data.

Profit + goods + data
Keep the goods, pocket the profit, and stash or sell the victim's personal data.

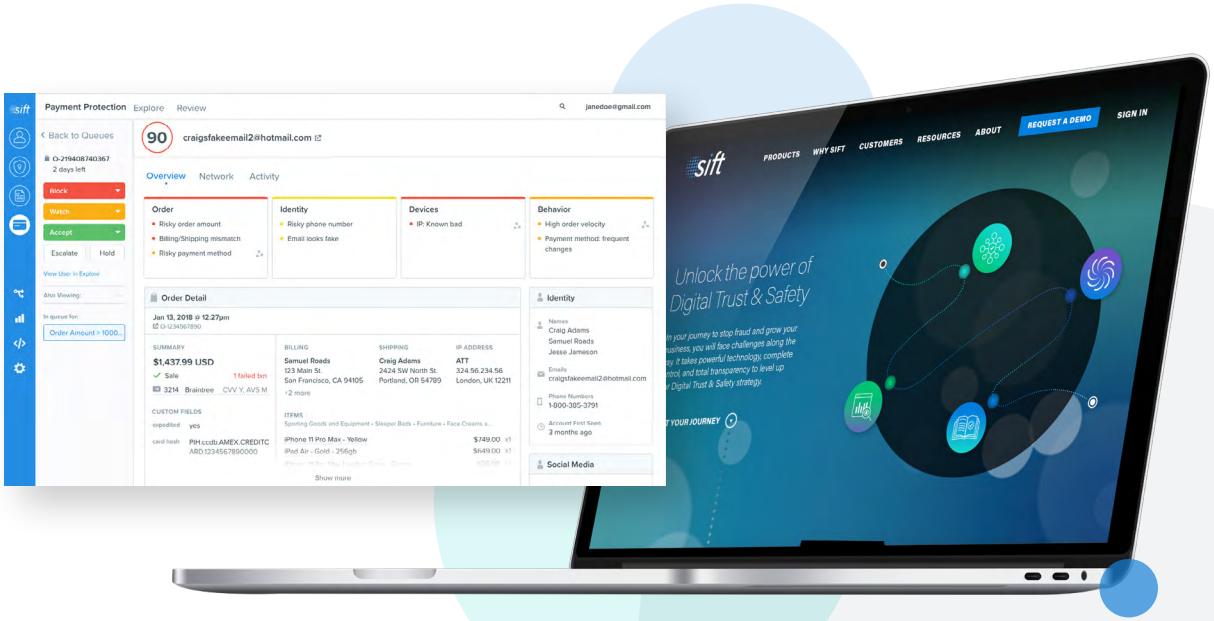
Exponential profit + goods + data
"Sell" goods to several buyers for profit and exploit the victims' personal data.

61% of consumer respondents say the #1 giveaway that something is a scam is an offer that appears "too good to be true."

Two-way marketplaces rose in popularity during the height of the pandemic, and are known to be especially vulnerable to this type of organized, multi-person content fraud. Part of their appeal for legitimate users is their partial anonymity and no-questions-asked nature; these same qualities are highly attractive to criminals with stolen goods to sell, promotions to abuse, and phishing links to distribute. Creating a profile is usually simple, verification steps can be bypassed with stolen information, and communications and sales between users happen without direct involvement from the merchant.

Last year, Sift's Data Science team identified a card-testing ring operating on a popular marketplace; earlier this year, they also surfaced a scheme on Telegram's public chat forums, in which fraudsters were linking up to purchase discounted food and beverage orders on behalf of customers using stolen payment information. Most recently, the team uncovered a sophisticated fraud ring leveraging guest checkout options on donation sites in an attempt to launder stolen payment information. With online giving spiking by more than 20% since COVID-19 hit, it's no surprise—criminals always follow the money.

Fraudsters continue to adapt ahead of the still-changing market, rendering static and reactive approaches to fraud prevention unfit to support growing e-commerce businesses. Trust and safety teams need an end-to-end solution that considers all types of abuse—including spam and scams—that can surface incidents and stop attacks in real time, without gutting growth.



Industry-leading machine learning trusted by leading brands

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, HelloFresh, and Twitter rely on Sift to catalyze growth and stop fraud before it starts. Visit us at sift.com , or follow us on LinkedIn.

Stay tuned for our next Digital Trust & Safety Index report to explore new online merchant and consumer data, developing e-commerce fraud trends, and expert insights. You can also access our Q1 2021 report on payment fraud on our website.