sift

## Q3 2021 DIGITAL TRUST & SAFETY INDEX

# Battling the new breed of account takeover fraud

Contents



ADAPT OR COLLAPSE

# Natural selection in the Fraud Economy

Fraudsters see global disruption as an opportunity. When the pandemic brought the physical world to a grinding halt in 2020, they seized the moment: eighteen months of peaks and valleys in online transactions gave them new places to hide, far more data to steal, and a growing number of dormant accounts to take over and exploit.

This digital acceleration hit businesses hard. Many companies ended up in a race they weren't prepared to join, and fell behind the competition. Others enjoyed profitable, sustained swells in transactions that drove rapid growth—growth that invited increased attention from a Fraud Economy rife with cybercriminals who are focused on optimizing existing abuse tactics, while at the same time developing more sophisticated ways to use them.


**of fraud blocked by Sift in Q2 2021 was ATO.**

Those abuse tactics often center around account takeover (ATO), which made up **39%** of all blocked fraud across Sift's network in Q2 of 2021, and is quickly evolving to be more diverse and popular with cybercriminals. And though ATO is more than a pathway to financial theft, trust and safety teams often consider it a downstream problem to be addressed only if and when payment abuse, unauthorized transactions, or similar activities occur—failing to act in the seemingly quiet period of time between the initial takeover and any clear signals of fraud.

Fraudsters are keenly aware that this is often how ATO is handled by merchants. They understand that it can take a backseat until the attack is already in motion, and are exploiting that knowledge to do scalable damage; hijacking users' credentials and loyalty points to sell on the dark web is only one piece of the puzzle. To succeed against evolving ATO, trust and safety teams will need to quantify its influence on all aspects of their business—including how idly allowing customers' accounts to become testing grounds for fraud can result in significant revenue loss, churn, and disputes.

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 1,000+ consumers surveyed in July and August of 2021.* This data illustrates the rapid, ongoing evolution of account takeover abuse and its spreading impact throughout digital commerce.


**Account takeover fraud skyrocketed by over 3x between Q2 2019 and Q2 2021.**

*On behalf of Sift, Researchscape International polled 1,063 adults (aged 18+) across the United States via online survey in July and August 2021.*

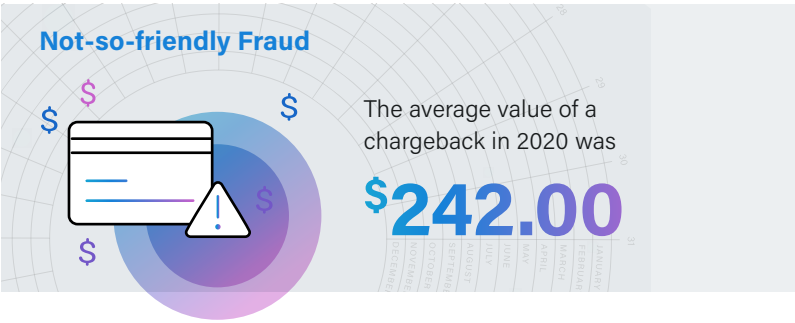
LAND & EXPAND ATO

# Emerging trends and consumer insights

Even as cybercriminals shift their focus towards optimizing existing tactics, the dark web plays a critical role in ATO's ever-growing popularity. Verified and "OG" (original) accounts are some of the most valuable items sold and traded by fraudsters online, and according to recent reports, can inspire extortion, blackmail, and harassment among the criminals vying for them. That's likely because the singular profit that these accounts can generate by sale alone is only part of what they're really worth.

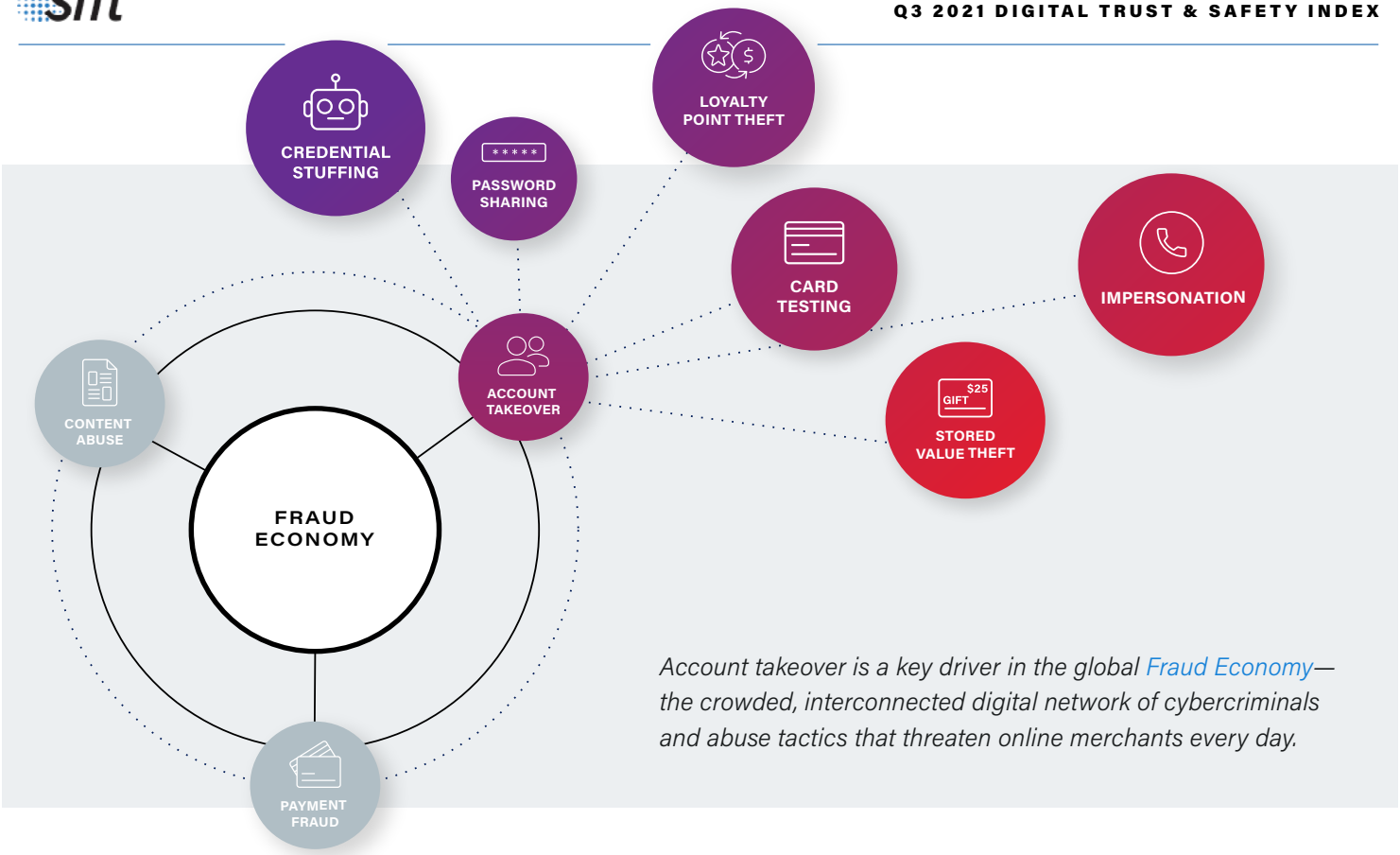
More often than not, nothing happens to corrupted accounts immediately after they've been hacked—no unauthorized purchases, no stolen loyalty points, and no attempts to update passwords. And that's because they're being used for something even more valuable: active accounts offer the most prolonged cover for fraudsters to perform card testing, as well as test the user's credentials across their other high-value accounts, which may use the same information. Fraudsters can use this veiled position to verify associated addresses and other personal customer data, correlate security codes and password hints, discover other cards on file to target, and reveal connected accounts or apps—all without making a purchase or otherwise tipping their hand.

Compared to 2019, last year's **2.8x surge in account takeover fraud** was one of the more significant results of the rising cyberattacks and unpredictable transaction volumes that defined year one with COVID-19. More than halfway through 2021, account takeover is still climbing: fraud rates have yet to dip back down to pre-pandemic levels, resulting in a meteoric **307% increase in blocked account takeover fraud between April 2019 and June 2021** across the entire Sift network.




As fraudsters continue to stockpile stolen account credentials, the potential for damage compounds, leaving businesses and consumers unaware of when the next attack will hit. This delay in action is precisely why ATO can be so destructive, buying fraudsters valuable time to launch credential stuffing and bot attacks as a means to infiltrate associated accounts and maximize profits. To help manage their growing list of ATO victims, many cybercriminals turn to the "All-In-One Checker" (AIO)—a popular tool among fraudsters to build databases of targets and then sell the account information through the dark web.


A recent study of Fortune 500 data breaches revealed that, no matter the industry, the most commonly used employee passphrase in every incident was, unbelievably, "password." Research from LastPass shows that **65% of people globally use the same password for every account they own**; 33% rotate a limited set of passwords across all accounts.




*Account takeover is a key driver in the global Fraud Economy—the crowded, interconnected digital network of cybercriminals and abuse tactics that threaten online merchants every day.*

## ATO by Proxy: When technology and tactics collide

Sift's Data Science team recently identified a prime example of ATO's ballooning risk, and how sophisticated and widespread fraudsters' automation tactics have become, after uncovering a global fraud ring—dubbed Proxy Phantom by Sift—in which fraudsters launched ATO attacks against dozens of e-commerce merchants through a massive credential stuffing campaign. The attack demonstrated how cybercriminals have remodeled typical ATO techniques to make a greater impact: using bots, proxy servers, and millions of compromised credentials, they were able to cycle through millions of usernames and passwords, while simultaneously and rapidly switching IP addresses in order to hide the origin of the attacks—and avoid getting blocked by typical rules-based fraud prevention systems. **In fact, the largest group—or cluster—of blocked IP addresses grew by 50x between Q1-Q2 2021.**

While it's inevitable that IP clusters (networks of connected IPs) will grow over time, this specific one exploded in size; in analyzing its traffic, our Data Scientists discovered that the cluster was centered around just a few proxy servers, and connected to scores of attempted, failed logins—pointing to automation and proxy IP rotation within the same address space. Essentially, these interconnected fraudsters were forcing merchants to play a supercharged, around-the-world game of whack-a-mole with new combinations of IP addresses and credentials (likely purchased in bulk on the dark web) coming for them at a cyclone pace.

Using automation to cycle through vast combinations of proxy IP addresses and stolen credentials, they attempted multiple, rapid fraudulent logins in the hopes of overwhelming security systems. These types of next-gen attacks could crush a merchant using a typical rules-based approach to fraud prevention, leaving them stuck trying to block one IP address after another and trying to catch up to a machine that rotates data faster than any human or static rules could. Worse, it could overwhelm those rules—**as more IPs show up and fail at breakneck speed, rules designed to assess risk will begin to identify everything as suspicious, deeply undermining the accuracy of the system**.

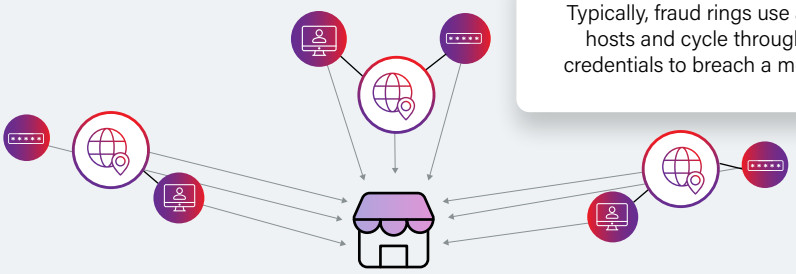
# Proxy Phantom:

## How fraud bots pirated profitable data for a global ATO blitz

*As normalcy faded and the pandemic raged on, the digital landscape exploded with an influx of companies scrambling to meet changing demands. But with this acceleration came innovation from cybercriminals, who began applying cutting-edge automation to speed up and broaden attacks. Enter Proxy Phantom, a ring of sophisticated fraudsters surfaced and stopped by Sift that used bots to deploy sweeping, large-scale ATO attacks against e-commerce merchants across the globe.*

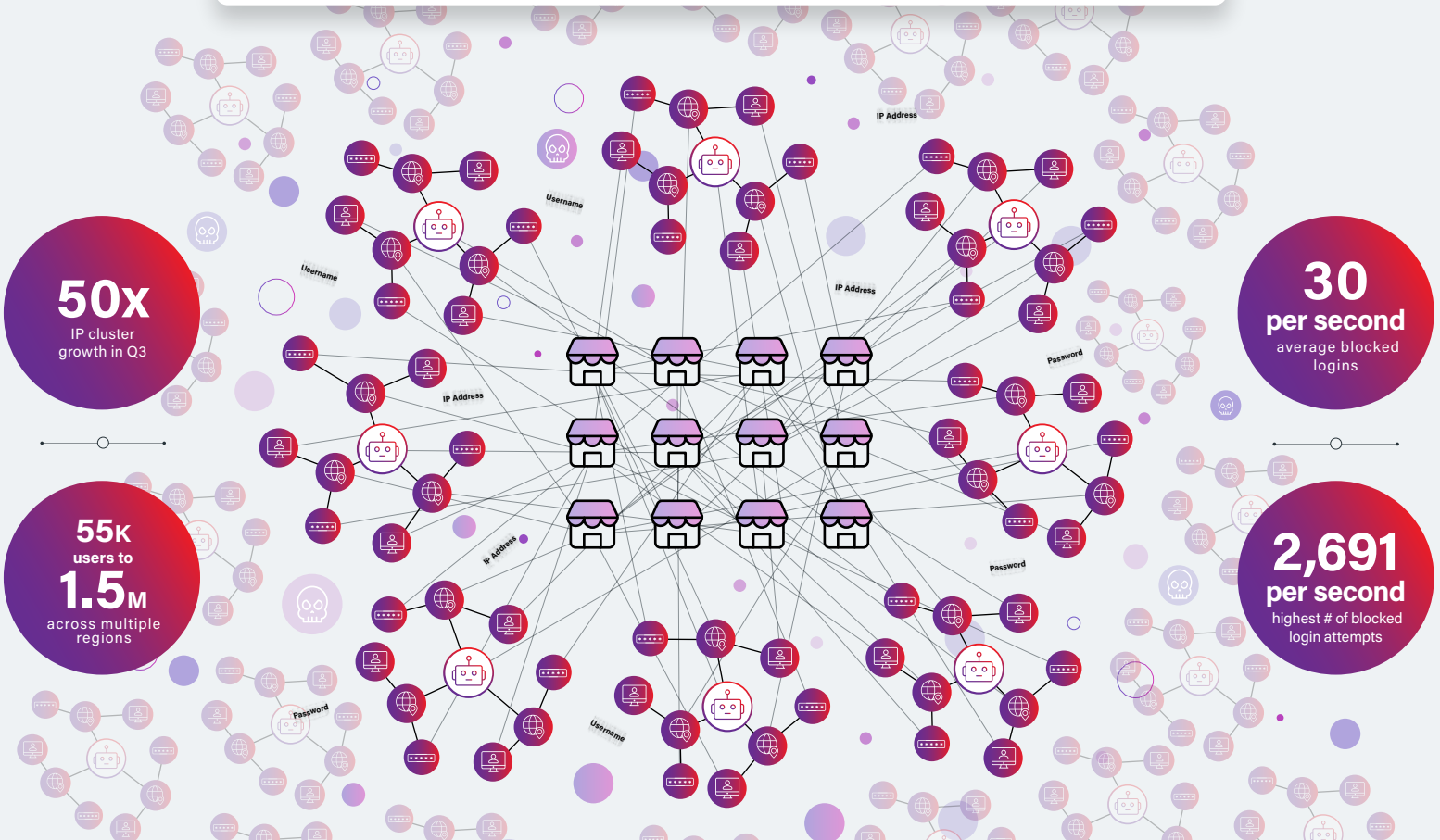
**IP Address** **Username** **Password**

In Q3 2021, Sift's Data Scientists identified and blocked an attack coming from multiple large IP clusters (related groups of internet protocol addresses) across our global network, primarily targeting digital goods/services and marketplaces—many from a known, high-risk ISP, and indicating a fraud ring in action.



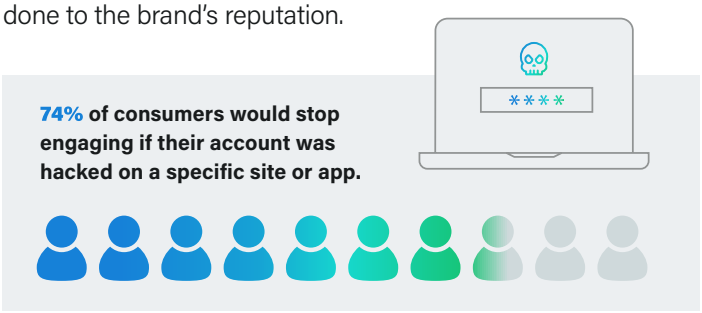
Typically, fraud rings use a handful of IP addresses or hosts and cycle through a large list of stolen user credentials to breach a merchant's security measures.

By leveraging automation for both credential and IP address rotation, this ring—dubbed Proxy Phantom by Sift—exhibited a major evolution of the classic blitz ATO attack, attempting an avalanche of rapid account takeover attacks against multiple businesses at once.



## Consumers react to online risk

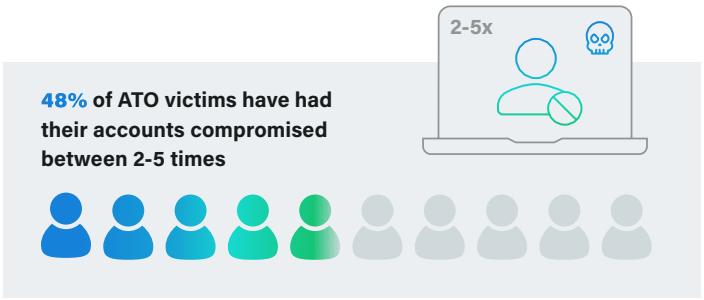
Not every account takeover attack will arrive with the menace and power of a global fraud ring behind it, but each incident does have the potential to cause churn. At worst, they can cost a business the victims' lifetime value (LTV), exponentially driving up customer acquisition costs (CAC), and resulting in further spending to gain new customers or alleviate damage done to the brand's reputation.




Even for defrauded customers that do not churn, there are negative material impacts to both the top and bottom lines of a business plagued by ATO. Remediation procedures are often manual, requiring a significant amount of time to resolve, and impeding the scalability of fraud operations.

Of customers surveyed by Sift, one-fourth of ATO victims claim the attacks occurred on financial services apps or sites. Nearly half of account takeover victims (**45%**) had money stolen from them directly, while **42%** had a stored credit card or other payment type used to make unauthorized purchases. Around one-third (**26%**) lost loyalty credits and rewards points to fraudsters, with **19%** of victims unsure of the total consequences of their accounts being compromised.

It's incredibly common for account takeover victims to have their information hijacked and tested across multiple sites;

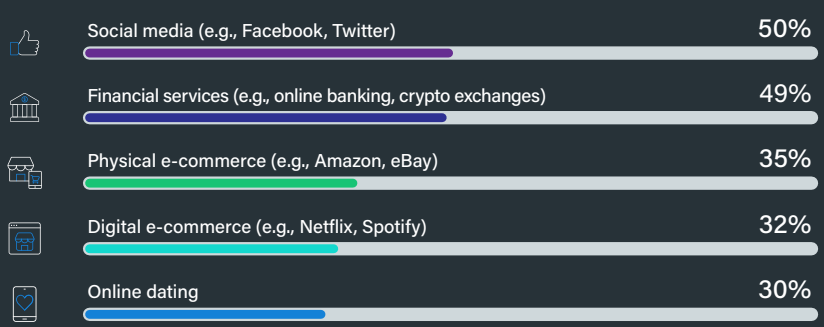



typically, anything cybercriminals can find that's associated with a person's name, email, password, phone number, address, or other exposed details. This breadth of personal information expands the fraudster's access to an individual's data and additional online accounts, *and* grows their card-and-credentials testing pool—a problem exacerbated by consumers' generally poor password hygiene and merchants' prioritization of speed over security in the user journey.

In addition to reusing or rotating the same passwords across accounts, **56%** of consumers say that they store their personal and payment details with various online sites and apps. It's surprisingly easy for fraudsters to stitch together a complete consumer profile and identify where people go online, making data breaches exponentially more valuable for fraudsters, and motivating them to execute ATOs without sounding any alarms.

It's the Fraud Economy's equivalent of a giant wooden horse packed with soldiers: a scaling network of increasingly specialized criminals using automation to overwhelm fraud prevention efforts, and develop more destructive and covert methods of ATO. And like the legendary Trojan army, they're already inside, waiting to strike.

### Where Consumers Feel Most at Risk




**JANE LEE**, *Trust and Safety Architect at Sift*

"Hacked accounts that go unflagged until a clear signal of fraud is surfaced could prove the most dangerous to consumers and businesses alike. That's because hacked accounts with no obvious fraudulent activity—like multiple password changes or unauthorized purchases—are unlikely to be caught by rules and reviewers right away, and even less likely to be flagged by customers."

GENERATION ATO

# Fighting organized abuse and automated attacks

While no industry has escaped evolving fraud or pandemic-driven unpredictability, fintech, digital goods and services, and omnichannel retailers are feeling the brunt of it in 2021. Account takeover fraud is up year-over-year across all of them; no real surprise, considering last year's mass migration to digital. But the magnitude of these industries in the market paints a troubling picture, with ATO rates continuing to rise well into the digital acceleration. As consumers traded in their physical bank branches for digital-first financial services and alternative payments like cryptocurrencies, fraudsters preyed on the lack of consumer education and protections associated with these digital accounts.

According to Sift's Data Scientists, those changes placed the fintech industry directly in the Fraud Economy's crosshairs during Q2 2021, leading to a massive surge in concentrated attacks aimed at crypto exchanges and digital wallets between April-June of this year. This springtime assault drove the **global ATO attack rate* up by 850% across fintech companies between Q2 2020 and Q2 2021.**

*The percent of blocked login attempts out of total login attempts.

### 2021 Top Targets: 3 highest ATO rates by vertical

*Fintech, digital goods and services, and retail saw significant YoY increases in account takeover rates.*



## Fraudsters Bank on Fintech

Every financial company is a fintech company in today's digital market, with long-established traditional banks investing in new technologies and cutting-edge crypto exchanges redefining how people interact with their finances.

And with the industry valued at $5.5 trillion, fraudsters are flocking: between Q2 2020-Q2 2021, **account takeover fraud exploded by 850%**, with the vast majority of attacks concentrated in crypto and digital wallets. In fact, over $1.9 billion was lost to cryptocurrency crime in 2020.

But fintech companies don't just need to reimagine risk to preserve profits now—they need to consider the potential, future value lost when fraud hits and leads to brand abandonment and churn. Nearly half of consumers (**49%**) already feel most at risk of ATO on financial services sites, and of account takeover victims surveyed, **25%** were defrauded while using online banking, digital wallets, crypto trading services, or similar apps and sites.

As consumers and fraudsters continue flocking to fintech, businesses must be prepared to protect customers' accounts while meeting their expectations for a seamless user experience. Adding points of friction and inflexible rules for trusted customers can risk driving them to competitors.

These outdated rules-based systems provide a linear approach to a non-linear problem, using fixed risk thresholds, too much friction, manual review, and broad signals that only catch some fraud—while trapping legitimate users in the net.

Fraudsters will never stop adapting vectors and strategies, or hunting for security vulnerabilities in e-commerce. To proactively secure customer accounts and fuel growth, trust and safety teams need holistic risk assessment methods and an end-to-end solution to accurately surface and stop account takeover fraud before it sneaks through the gate.


## Evolve your fraud solution with 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, HelloFresh, and Twilio 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 final 2021 Digital Trust & Safety Index report to explore new online merchant and consumer data, developing fraud and dispute trends, and expert insights. You can also visit our website to access previous Sift data reports, including our Q1 dive into payment abuse and our Q2 coverage of spam, scams, and content fraud.