sift

Q3 2022 DIGITAL TRUST & SAFETY INDEX

Account takeover data, trends, and insights

Contents

Account takeover fraud (ATO) evolves so rapidly that reacting after it's happened is about as effective as doing nothing at all. But doing nothing about account security is not an option for any business—particularly as ongoing economic disruption causes unforseen challenges across markets, and creates new pathways for fraudsters to inflitrate user accounts.

To proactively prevent fraud and eliminate security blindspots, businesses need intelligent automation built on real-time insights. But effective account security in a fluid economy takes more than tools. Risk teams need actionable, adaptable strategies in place to outpace evolving fraud, scale operations, and improve risk assessments across the user journey.

The findings in this report illustrate rising ATO attacks across industries YoY (H1 2021 versus H1 2022), with proprietary insights from surveyed consumers* and data from Sift's global network of 34K+ sites and apps comprising 70B monthly events.

H1 2022 DATA

Accelerated ATO weakens consumer trust

ATO acts as a key pillar in the global Fraud Economy, powering payment abuse and content scams by adding apparent legitimacy to fraudulent transactions and posts. It gets fraudsters behind the gates, where they can either remain dormant and wait for profitable opportunities to arise—or immediately hijack anything of value before disappearing back into the dark web to sell the data they've stolen.

In H1 2022, account takeover fraud spiked **131% YoY** across the entire Sift network, with fintech and marketplaces shouldering painful increases of their own.

Consumers surveyed by Sift report frequent encounters with account takeover—**44% of reported victims have experienced ATO up to five times**, with over half of those impacted unaware their accounts had been compromised until they logged in and noticed unfamiliar activity or missing funds and credits.

Rising ATO across Sift's global network 2021-2022

All network	↗ **131%**
Fintech	↗ **71%**
Marketplaces	↗ **39%**
On-demand services	↗ **34%**
Digital goods & services	↗ **9%**

*On behalf of Sift, Researchscape International polled 1,105 adults (aged 18+) across the United States via online survey in July 2022.

Failing to notify users that their information has been exposed due to ATO is a critical miss for businesses looking to maintain user trust and protect revenue. Without immediate awareness of an account takeover, businesses and affected users can't take action to stop the threat from spreading—and the merchant can expect to eat the cost of any associated losses.

Opportunity favors fraudsters who attack poorly secured accounts. They're granted the freedom to use customer data and stored value over time, and stay undetected while they do it. They can use that camouflage to test hijacked credit cards, or infiltrate other accounts connected to those same compromised credentials—even on completely different sites and apps where the user owns a login. Worse, they'll quickly realize that no one, and nothing, is coming to stop them.

Every vertical faces evolving fraud, but consumers perceive a select few as particularly high-risk. Well **over one-third of survey respondents** pegged financial services and digital goods providers as riskiest for ATO.

The aftermath of ATO

51% of victims only discovered ATO after logging into their account and noticing suspicious activity.

42% of victims had unauthorized purchases made on the impacted site using stored payment info.

30% of victims lost rewards points or credits.

This potential for account fraud isn't enough to keep people away from these types of sites. Successful attacks, on the other hand, drive customers to competitors:

well over one-third of consumers would stop engaging with the jeopardized brand completely and seek out another provider.

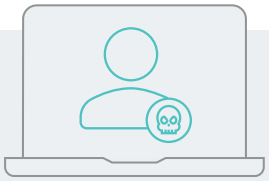
Many victims of account takeover are targeted on sites they visit most frequently*

*Respondents could select multiple answers.

According to recent reports, the top consequences of ATO in 2021 included fraudulent credit card transactions and funds being drained from person-to-person (P2P) accounts on platforms like PayPal and Venmo.

But the material losses of account takeover don't end with a couple of chargebacks and reinstated loyalty points. Consumers understand that fraudsters are after their money and information, and expect that online merchants will secure both. When they don't, it signals to victims that the site or app is unsafe, leading to attrition, negative reviews, bad press, lost partnerships, and industry-wide distrust. For merchants, ATO leads to sinking profits, shrinking customer lifetime value (LTV), and inflated acquisition costs (CAC).

43% of consumers would stop using a site or app if their associated accounts were compromised by ATO.



KEY INDUSTRY TRENDS

Fintech stays fixed in the crosshairs

Financial tech providers continue to feel the impact of digital transformation. Mobile banking and decentralized finance have built fintech into a $112.5B industry as of 2021, with the global market expected to reach $332.5B by 2028.

No one pays closer attention to that kind of consumer cash flow than fraudsters—crypto scammers alone siphoned a record $14B in 2021. And, because consumers now enjoy instant access to banking, transfer, and payment options, the window of opportunity fraudsters have to attack is short—but highly valuable, and therefore attractive.

Earlier this year, Sift reported surging average daily transaction volumes across fintech, up **121%** YoY—promising growth that drew first-time investors, and seasoned cybercriminals, to new avenues for fraud.

This year's crypto downturn provides an ideal space for ATO to fester. Hefty losses and unrealized investments mean fewer people are actively monitoring their accounts. That makes it easier for fraudsters to go undetected—much like travel and entertainment vendors saw at the height of pandemic shutdowns—ushering in additional risk when takeovers aren't immediately identified and stopped.

Crypto's growing volatility has led some merchants in the space to submit master account requests to the Federal Reserve. If granted, these accounts allow exchanges to access and benefit from the same protections awarded to traditional banks. Primarily, it enables direct access to the Federal Reserve's payment systems, and grants opportunities to settle transactions with other participants in central bank money.

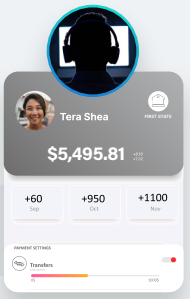
Fraudsters Bank on ATO: Rising account takeover 2021-2022

The heightened concern is warranted. Recently, Sift's Trust and Safety Architects uncovered a new iteration of the classic cashout scam, where fraudsters work together to access and drain value from exposed bank accounts. In the unregulated crypto space, they make use of each other's specialized skills to hack accounts and funds, eventually striking bitcoin before splitting the payout and parting ways.

BRITTANY ALLEN, *Sift Trust and Safety Architect*

Account takeover attacks are proving to be a primary attack method among fraudsters in our challenging economic environment. Adding insult to injury, cybercriminals are leveraging automation via bots and scripts to launch ATO attacks at scale, often forcing businesses to choose between introducing excessive friction in their user experience or being consumed by fraud. However, businesses that adopt a Digital Trust & Safety strategy—one that allows businesses to introduce friction dynamically—can stifle fraudsters without treating customers like criminals.

Crypto Cashout: When fraudsters join forces



1

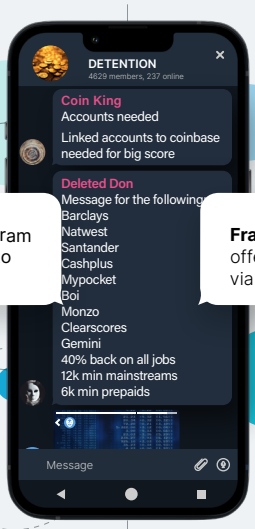
Fraudsters access stolen funds and accounts

Fraudster A has access to hijacked or illicitly-obtained funds.

Fraudster B takes over bank, crypto wallet, and crypto exchange accounts.

2

Fraudsters link up

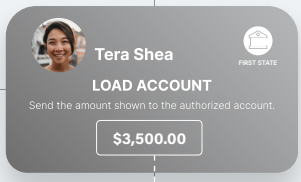


Fraudster A solicits on Telegram for combined bank and crypto account access.

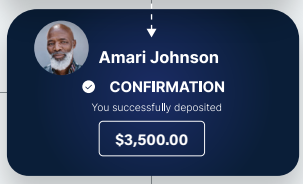
Fraudster B responds with an offer to work together, typically via direct message.

3

Transfer stolen funds



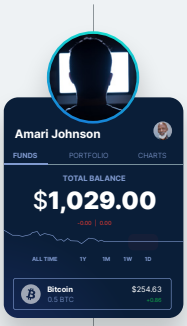
Fraudster A loads the stolen funds into Fraudster B's bank account.



Fraudster B transfers the funds into a stolen crypto exchange account or wallet.

4

Drain funds and split the profits



Fraudster B withdraws funds from the crypto account to a private wallet.

+ $1,750.00

Fraudsters split the profits.

+ $1,750.00

New research shows that the projected, cumulative merchant losses to online fraud will exceed $343B globally between 2023 and 2027. Trust and safety teams must adopt an end-to-end, real-time approach to outpace evolving abuse while keeping up with changing customer demand.

Sift's Digital Trust & Safety Platform is backed by a network of billions of events and intelligent automation at every touchpoint, allowing fraud analysts to succeed and scale while propelling business growth with every transaction. Take our Digital Trust & Safety Assessment today, and get actionable advice on your specific fraud challenges and growth opportunities from our team of industry experts.

Proactively prevent all types of fraud 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 all types of online fraud and abuse with intelligent automation that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including DoorDash, Blockchain.com, and Twitter rely on Sift to catalyze growth and stop fraud before it starts. Visit us at sift.com, or follow us on LinkedIn.