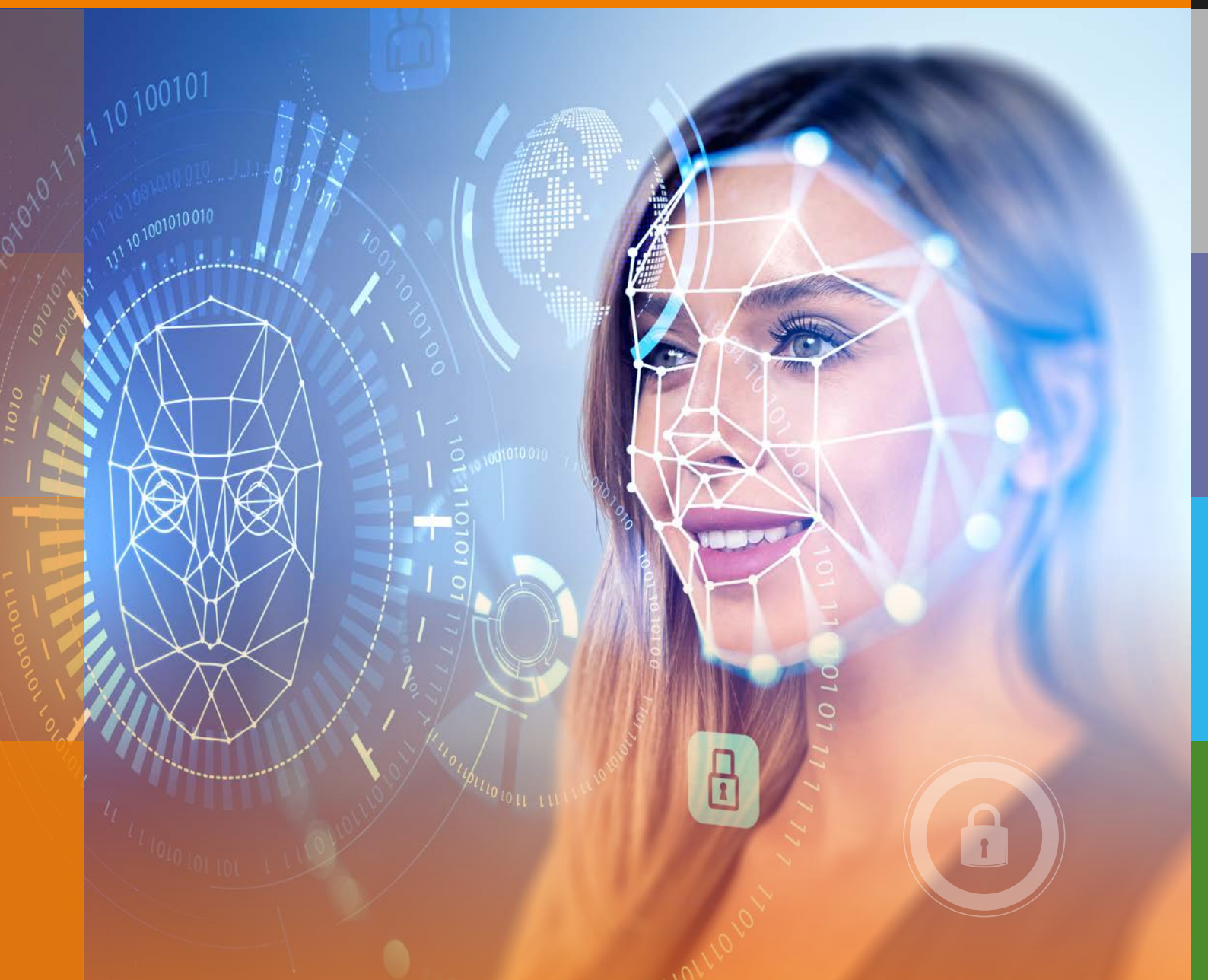


# Fraud Prevention in Ecommerce Report 2023-2024

Keeping Fraudsters Out While Balancing a Seamless Customer UX



Endorsement partners:



Key media partner:



Sift Trust & Safety Architect, Rebecca Alter, shares how businesses can successfully shut down account takeovers and evolve fraud operations to meet the pace of a dynamic global market.



**Rebecca** is a risk operations professional with extensive experience building teams and developing processes. She is also a strategic thinker who creates interdepartmental alliances and partnerships. She excels in a fast-paced, startup environment where there's an opportunity to lead, build teams, develop processes, and find efficiencies.

Rebecca Alter ■ Trust & Safety Architect ■ Sift

## What factors have contributed to the significant rise in ATO, as indicated by the 354% YoY increase across Sift's network in Q2 2023? What does it mean for businesses?

The problem we are facing now is that fraudsters don't have to hack into accounts when they can just use stolen credentials to log into them instead. Purchasing validated, stolen credentials online can be easier and faster than creating fake accounts or phishing campaigns, and more profitable to bad actors more quickly. With the availability of **automation-backed credential stuffing tools**, the entire process of account takeover is more efficient and scalable. The massive year-over-year rise in ATO attacks is motivated primarily by a desire for increased access to data that can enable a payout. It's further fuelled by the rising democratisation of fraud, widespread and constant use of social media platforms, and ongoing evolution of attack techniques. The speed of fraud complicates the fight, especially with the introduction of consumer AI tools and other advancements hitting the market every day. Phishing and social engineering tactics have become more convincing and harder to detect, making it easier for attackers to trick users into revealing sensitive info. For businesses, it's the usual suspects that make ATO so damaging: increased financial losses and disputes, stunted growth, and customer churn on a massive scale—**76%** of consumers surveyed by Sift would stop

using a website or app permanently due to ATO. Moreover, **18%** of consumers surveyed by Sift have experienced account takeovers, with **62%** taking place in the past year. Adding to the overall cost, businesses that fail to adequately protect customer data can face long-term legal consequences and regulatory fines that can't be recouped.

## How does the democratisation of fraud tie into ATO-as-a-Service, and what implications does it have on companies and consumers?

The **democratisation of fraud** means that anyone with Internet access can engage in fraudulent activities. Professional fraudsters still represent the largest threat to digital businesses, but consumer participation in illicit activities is growing, contributing to the overall impact of ATO across industries. Our most recent survey revealed that **14%** of consumers know someone who has intentionally committed account takeover fraud, with **4%** having committed ATO themselves.

“Professional fraudsters still represent the largest threat to digital businesses, but consumer participation in illicit activities is growing.”

The blurring lines between violator and victim aren't a big surprise for those who spend time tracking fraud. Cybercriminals are increasingly climbing up out of the dark web and openly using major social platforms like TikTok and Instagram to attract new recruits. →

After hooking first-time fraudsters, they'll push them off-platform to messaging apps like Telegram, where stolen credentials and Fraud-as-a-Service schemes are being advertised. We recently uncovered conversations surrounding one automated Fraud-as-a-Service tool via Telegram. Known as *Atlantis X* (formerly Atlantis AIO), this credential-stuffing script is accessible through a link and priced at USD 150. It allows fraudsters to test the validity of compromised credentials against various businesses, quickly and at scale. What makes Atlantis X unique is its regularly updated list of supported sites, along with tactics in place to prevent the tool from being blocked by targeted companies. Fraudsters can easily take Atlantis-authenticated data to compromised websites and apps, accessing accounts and whatever loyalty points, discounts, funds, or other data is stored behind the gate—without setting off any alarms.

### Are there specific industries or sectors that are more vulnerable to ATO attacks, and if so, why?

Some industries, such as fintech and food & beverage, saw a disproportionate increase in ATO attacks YoY. The food & beverage space was slammed with a 485% uptick in account takeover, reflecting snowballing fraud in the market that began during the COVID-19 pandemic lockdown. Fintech was hit with an 808% YoY increase in ATO, with attacks in industry sub-verticals like loyalty and crypto surging 890% and 189%, respectively. Moreover, many fintechs are still not regulated like traditional banks, so compliance and security don't necessarily stack up against the threat of digital fraud. The tradeoff is innovation; fintechs can go after expedient growth, globalise transactions and be agile in ways not available to classic financial institutions.

### What have Sift Trust & Safety Architects observed regarding the collaboration among fraudsters in exchanging tools and tips for stolen data?

Fraudsters have been exchanging tools, tips, and opportunities for acquiring stolen data online for years, and not just in hard-to-reach corners of the Internet. Software, scripts, strategy - nothing is

off-limits, and there's a concerning level of coordination and cooperation within the **Fraud Economy**, allowing cybercriminals to streamline their own operations and make their attacks more efficient and effective.

Knowledge-sharing and coordination on attack methods suggest that fraudsters are also actively working together to identify vulnerabilities in systems and networks, amplifying the threat they pose. 24% of consumers report seeing offers to participate in account takeover schemes online, and that's just what's floated to the public surface. Fraudsters of all persuasions can easily find each other on popular messaging apps — our latest **Digital Trust & Safety Index** report highlights one example of a well-known bad actor whose Telegram channel boasts over 20,000 subscribers.

### What are some practical examples of how businesses can evolve their fraud operations to keep pace with the dynamic global market?

Scaling and adapting fraud operations while a business grows presents challenges beyond security. Many companies start with point solutions to address specific stages of the user journey they're most concerned about — like 2FA to protect login, CAPTCHA to verify, or a payments-only platform that protects transactions but doesn't handle disputes. But for businesses to reach their most sophisticated state of operations to effectively combat multiple types of fraud at scale, they need integrated protection from checkout to chargeback.


By implementing advanced technologies such as machine learning and AI, behavioural analytics, and biometrics, businesses can focus on accuracy and order acceptance instead of manual review. Continuous monitoring, multi-factor authentication, and data enrichment are also crucial for real-time fraud detection, and leading companies should build those elements into fraud prevention from the start.

[Click here for the company profile](#)



[sift.com](https://sift.com)

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivalled global data network of one trillion (1T) events per year, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Twitter/X, and Poshmark rely on Sift to gain a competitive advantage in their markets. Visit us at [sift.com](https://sift.com), and follow us on LinkedIn.

Company		Sift	
		<p>Sift is the leader in Digital Trust &amp; Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of one trillion (1T) events per year, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Poshmark, and Twitter rely on Sift to gain a competitive advantage in their markets. Visit us at <a href="https://sift.com">sift.com</a>, and follow us on <a href="#">LinkedIn</a>.</p>	
<b>Background information</b>			
Year founded	2011		
Website	<a href="https://sift.com">sift.com</a>		
Target group	<ul style="list-style-type: none"> <li>• Merchants/ecommerce</li> <li>• PSPs/acquirers</li> <li>• SMBs</li> <li>• Corporate</li> <li>• Fintech</li> </ul>		
Supported regions	Global		
Contact	<a href="mailto:sales@sift.com">sales@sift.com</a>		
Company's tagline	Our mission: Help everyone trust the Internet		
Member of industry association and/or initiatives	Marketplace Risk, Merchant Risk Council, Merchant Advisory Group, The Fraud Practice		
<b>Core solution</b>			
Core solution/problems the company solves	<p>Fraud/risk management and decisioning platform</p> <p>Sift offers end-to-end fraud and risk mitigation solutions that secure each touchpoint of the customer journey.</p>		
<b>Technology</b>			
	Native cloud		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Small transaction verification	x		
Email verification	x		
Phone verification	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics	x		
Device fingerprinting	x		
Geo-location	x		
3-D Secure 2.0	x		
<b>Methodology</b>			
Machine learning	Rule-based Supervised ML		
<b>Decisioning</b>			
	Manual review Case management Decision orchestration		
<b>Chargeback management</b>			
	Chargeback dispute		

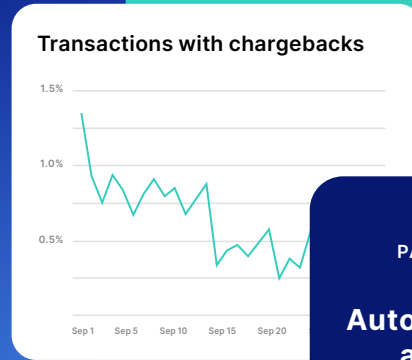
## Business model

Pricing model	Sift offers fixed minimums along with the 'per transaction' usage-based pricing based on the volume of billable events. The billable events are determined by product and use case
Fraud prevention partners	<a href="https://sift.com/partners">https://sift.com/partners</a>
Year over year growth rate	Privately held
Number of employees	Privately held
Future developments	Privately held
Customers	Box, Wayfair, Twilio, Uphold, Poshmark, Patreon, Reddit, Remitly, Hello Fresh, Tap Tap Send, Vestiaire Collective, Get Your Guide, Tier Mobility
Customers reference	<a href="https://resources.sift.com/case-studies/">https://resources.sift.com/case-studies/</a>
	<a href="#">View company profile in online database*</a>
	<p>*The data present at the time of publication may be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a>.</p>



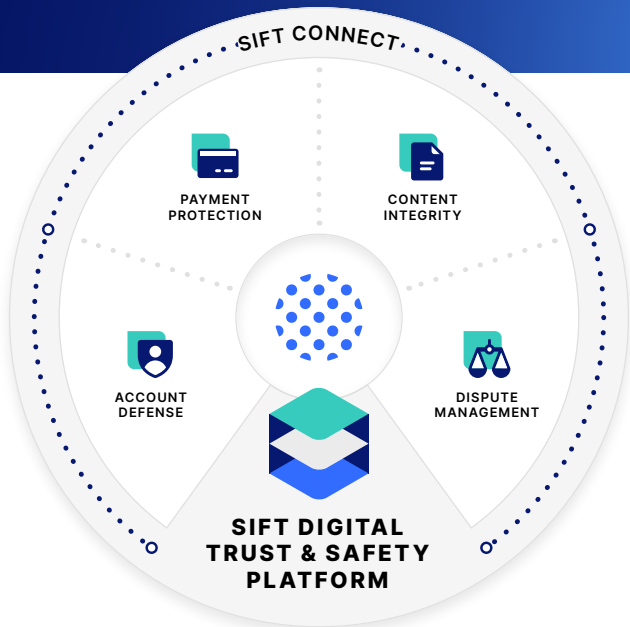
# Cut fraud losses by 90%

Proactively stop fraud and fuel growth from checkout to chargeback with the Sift Digital Trust & Safety Platform.




**PAYMENT PROTECTION**

**Automate on-demand authentication**



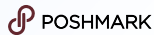
## A smarter, simpler way to stop fraud

Built with a single, intuitive console, Sift’s end-to-end solution eliminates the need for disconnected tools, single-purpose software, and incomplete insights that drain operational resources.

The Sift Digital Trust & Safety Platform does what other fraud tools can’t, adding connected data, adaptability, and intelligent automation to every aspect of risk operations.

## Leading brands rely on Digital Trust & Safety

Launch unbeatable defenses against current and future threats using accurate, real-time data from our global network of 1 trillion annual events, representing 34K sites and apps.



Visit [sift.com](https://sift.com) to learn more →