



**Merchant
Fraud
Journal**

ATO Fraud in Retail



Sponsored by

Ravelin

Table of Contents

3	Introduction
4	Fraud Prevention Leaders Answer the Question: What are the Biggest ATO Threats You Face?
4	An overview of ATO Attacks in the Retail Sector
6	How do Retail Fraud Prevention Leaders Prevent ATO Fraud?
8	What tactics do leaders use to prevent ATO attacks?
10	5 Key ATO Findings
13	About MFJ
12	About Ravelin

Introduction

This report draws insights from our recent online merchant survey, specifically focused on the threats and trends of account takeover fraud (otherwise referred to as ATO) in the retail sector.

Account takeovers are one of the fastest growing threats to online merchants, as half of survey-participants noticed an increase in the past year. But many businesses still underestimate the threat of ATO and lack an efficient management strategy. Our findings suggest that there are significant gaps in merchant defences that need to be filled.

This report provides insights into:

- Merchant perceptions of account takeovers and the business impact
- Tools, budgets and methods for monitoring account takeovers
- The macro environment impact

Survey Methodology

This quantitative survey was commissioned by Ravelin and carried out by Qualtrics using a panel of 1000 fraud professionals from countries around the world in 2020. Survey participants work for online merchant businesses with over \$50million in annual revenue. The survey was translated into each respondent's local market language for clarity.

Our survey participants are fraud and payments professionals from around the globe. These professionals work in key ecommerce markets in Europe, Australia, North and South America.

All participants work in a fraud-related role, from Fraud Analyst up to Chief Financial Officer. Two-thirds of participants come from senior roles, with over 40% at C-Level.

Fraud Prevention Leaders Answer the Question: What are the Biggest ATO Threats You Face?

Our survey revealed that **account takeover fraud increased for more merchants than other forms of fraud. Around half (48%) of merchants noticed ATO increase in 2020, and over one in ten reported a significant increase.**

We asked participants to rank the consequences of account takeover by the severity of risk they pose.

WHAT ARE THE BIGGEST ATO THREATS YOU FACE?

Level of importance	Revenue loss	Personal data theft and associated fines	Reputational damage	Time/operational cost of account recovery
1	36%	34%	18%	12%
2	28%	29%	26%	17%
3	24%	25%	28%	23%
4	12%	12%	28%	48%

ATO attacks are a huge customer experience issue. If customers can't trust that you are protecting their information, they will go somewhere where they feel more secure.

Head of fraud at a major online retailer.

An overview of ATO Attacks in the Retail Sector

Although the threats are similar, their effects vary from industry to industry. Below is a breakdown of how these challenges are manifesting themselves in actual, increased ATO attacks:

INCREASE IN RETAIL ATO ATTACKS

Increased	33%
Significantly increased	12%

AVERAGE NUMBER OF ATO ATTACKS PER MONTH

Most to least	Attacks p/month
Retail - Groceries	4.4
Retail - H&B	3.2
Retail - Fashion	2.8
Retail - Electronics	2.8
Retail - FMCG	2.8
Retail (total)	3.2

Merchant perception of ATO

Account takeover is the number one risk for a quarter of all merchants (25%), and is seen as a top risk for over two-thirds (70%). It is perceived as the second biggest fraud risk behind online payment fraud across all industry groups.

For retailers, the problem is even more acute:

INDUSTRY GROUP PERCEPTIONS OF ATO RISK

Total average no. 1 risk	29%
Total average no. 3 risk	72%

More retail businesses put ATO as their top risk (29%) and in their top 3 (72%) than other industries, despite reporting fewer average attacks than other groups. ATO ranks as the number one risk to the highest percentage of fashion retailers, with 32% putting it at the top, which is almost 10% over the survey-wide average.

ATO fraudsters target fashion merchant customer accounts as products are easy to bulk-buy and resell without raising suspicion. They can also game fashion ‘drops’ to their advantage, using bad bots to scrape account details, masked by genuine busy traffic. Fashion merchants are conscious of ATO’s revenue impact, as we later discuss, 44% ranked revenue loss the biggest concern, significantly over the survey average (36%).

Grocery merchants tend to underestimate the risk of ATO. Despite reporting to see the most attacks in this industry group, only 25% of grocery merchants ranked it as the no.1 risk, and just 65% put it in their top 3, which is notably under the retail average.

How do Retail Fraud Prevention Leaders Prevent ATO Fraud?

Next we asked how fraud leaders prevent ATO fraud. We covered two broad topics: 1) How leaders structure their ATO prevention teams; 2) The tactics they use to prevent individual ATO attacks

How do leaders structure their Retail Fraud ATO prevention teams?

We found that unlike chargeback fraud, multiple teams are often involved in ATO management. Overall, just over 60% of fraud teams manage ATO, leaving the responsibility to a range of other teams--from customer service to broader account/security teams--in 40% of businesses.

But teams are not always aligned, and can have competing priorities like security vs. conversion rate. Poor communication between teams, worsened by pandemic-driven remote working, can obstruct ATO management as the right people can't easily access key information. By the time payments teams notice an ATO chargeback, the damage may have already been done.

"Our IT dept recently detected a lot of credential stuffing, lots of super old accounts were suddenly logged into. It eventually got round to us." – Fraud Manager from an online dating business.

67%: The percentage of retail merchants that manage ATO

What tools do leaders use to prevent Retail Fraud ATO?

Online businesses use a combination of tools, and over half of every industry uses machine learning against fraud. But what are the key tools to protect against ATO?

Two-factor authentication at login

Two-factor authentication (2FA) at login is one of the most effective means of ATO prevention. Microsoft suggests it prevents 99.9% of cyberattacks from breaching accounts. Although 2FA adoption is increasing, merchants who aim for frictionless transactions can be reluctant.

When merchants have 2FA, the most commonly offered method is in-app authentication (53%) followed by one-time password (51%), human verification (36%) and finally security questions (24%). Security answers can be bought alongside breached credentials, so it's positive that this is not the default choice for 2FA.

When merchants have 2FA, the most commonly offered method is in-app authentication (53%) followed by one-time password (51%), human verification (36%) and finally security questions (24%). Security answers can be bought alongside breached credentials, so it's positive that this is not the default choice for 2FA.

Machine learning and 2FA complement each other. Fraud teams can enable a rule based on the model's prediction and trigger 2FA for any uncharacteristic login, increasing accuracy and reducing genuine customers blocked.

However, there are ways fraudsters can get around 2FA, including calling customer support services and using social engineering techniques to get the account phone number changed.

Phonecall verification

Just under half of merchants monitor phone call verification (49%), but our recent analysis of merchant ATO data shows that 90% of attackers change the account phone once successful. Perhaps fraud teams underestimate the value of this tool.

Machine learning

Machine learning is the most popular tool, used by 57% of merchants. Digital goods and marketplace merchants are most likely to use machine learning against fraud, particularly taxi/cab (65%) and gambling (60%). It's important to remember that whilst machine learning can be used to protect against online payment fraud, it can also be a powerful tool to detect and prevent ATO attacks.

Machine learning is useful to detect ATO as models can monitor behavioral changes on an account. This is key, as sophisticated fraudsters can now circumvent velocity-based ATO rules. Machine learning models base decisions on previous account activity. For example, the model can evaluate the likelihood that a certain customer will log in from a given location, IP address or device.

Device ID solutions

Around a third of survey-participants (32%) have no device ID tool. Device ID tools are key to spotting ATOs, as fraudsters often use the same device to try and access multiple genuine customer accounts.

But, a device ID solution isn't a silver bullet. Fraudsters can avoid detection by changing their device or IP address, and sometimes there's interference from browser regulations. This is why graph networks are a more powerful tool to detect links between accounts by more than just the device ID. Using a graph network you can quickly see when accounts become linked by contact details such as phone number or email.

Graph networks

It's concerning that under half of merchants use graph networks, these are a key method for detecting and preventing wide-scale ATO attacks. Graph networks highlight networks of accounts linked by shared data points, such as a device, phone number or email. This is commonly seen when a fraudster carries out an ATO attack or even if multiple fraudsters buy and use the same account details.

Type	Use of Graph networks	Device ID	Attacks p/month
Groceries	53%	31%	4.4%
H&B	42%	31%	3.2%
Fashion	41%	41%	2.8%
Electronics	42%	39%	2.8%
FMCG	43%	38%	2.8%

What tactics do leaders use to prevent ATO attacks?

Below, we discuss some of the main tactics respondents cited as tactics they use to prevent ATO attacks:

Customer activity monitoring

Account takeovers can be notoriously difficult to spot, but monitoring changes in customer behaviour is key to identifying successful attacks. Very few merchants are monitoring customer logins and new devices which is concerning, as these are the first points where account takeovers can be seen.

Type	Averages
Account email changes	67%
Account phone number changes	57%
Account phone number changes	56%
New activity on dormant accounts	51%
New devices used on an account	44%
Password changes	56%

The customer journey can also be thought of as the ‘fraudster journey’. Every interaction between you and your customers is a potential vulnerability to be exploited. The key is to not only monitor touchpoints at the end (checkout), but to build an understanding of how all your touchpoints interact to form a single, cohesive story for each and every order

Fraud prevention specialist at an enterprise retailer.



Account email change

Overall, 66% of merchants monitor account email changes – it is the most popular activity to monitor. It helps fraud teams identify ATO as some attackers change the account email address once they have access – according to our analysis of ATO data for a group of merchants, around 9–10% of attackers do this.

Account phone number changes

Account phone number changes are the second most popular activity fraud teams monitor, as 56% of all merchants track it. In our recent analysis of successful ATO attacks, 90% of attackers changed the account phone, and in 24% of cases, the phone number was changed twice or more. This suggests that it's more likely for attackers to change the phone number (24%) than the email address (9–10%) after taking over an account. Fraud teams should closely monitor both activities, not just email changes.

New activity on dormant accounts

Due to the long life-cycle of data breaches, account details can emerge on hacker forums well after the original breach, enabling ATOs on older accounts

Most fraudsters are impatient, so will not wait long to monetize an attack. But if there are notable differences between new behaviour and old account information, it's likely to be ATO.

New devices

New devices are the least monitored user activity by merchants (42%).

Customer logins

Around half (49%) of merchants monitor logins from a fraud perspective.

It's essential to monitor logins to understand how many ATO attacks your business is facing. Login rates – successful vs. failed – can help prove that account takeovers have happened. This data is vital for fraud teams hoping to gain C-level understanding and secure investment in ATO defences.

Acceptable customer login statistics look different depending on the business. Some merchants expect more genuine customers to forget passwords and attempt multiple logins than others. But monitoring logins makes credential stuffing easy to spot, as failed login rates will be abnormally high, often concentrated to one IP, user agent or device.

5 Key ATO Findings

Merchant responses to account takeovers in this report give us a valuable, in-depth understanding of the threat facing fraud teams today and in the future. The high-level insights highlight where further investigations can enable merchants to boost their ATO detection ability, and gain deeper knowledge on their customers.



Account takeover fraud increased for more merchants than any other fraud

ATO increased more than online payment fraud and friendly fraud last year. Digital goods merchants are heavily targeted.



Half of merchants have seen ATO increase in the past year

On average, merchants experience 3.5 high-impact ATOs every month.



Over two-thirds of merchants see ATO as a top 3 fraud risk

ATO is seen as the second biggest fraud risk behind online payment fraud. Revenue loss is considered the most important consequence of ATO. The impact of reputation damage and operational costs are underestimated.



Not enough merchants use device ID solutions and graph networks

Only a third of merchants use device ID solutions and under half use graph networks. Machine learning and breached credential bases are widely used, but are not silver bullets. 2FA is effective at blocking ATO but many businesses are reluctant to create friction.



Too few merchants monitor customer activity

Around half of merchants do not monitor logins from a fraud perspective, and less than half monitor new devices.

This report presents the survey data from retailers. Additional information about digital goods, marketplaces, and travel and hospitality merchants can be found by downloading our full report.

About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.



About Ravelin

Ravelin provides technology and support to help online businesses prevent evolving fraud threats and accept payments with confidence. Combining machine-learning and graph network visualisation, Ravelin helps businesses draw deeper insights from their customer data to detect fraud, account takeover and promotion abuse and increase payment acceptance.




Contact Merchant Fraud Journal

Editor In Chief - Bradley Chalupski
Bradley@merchantfraudjournal.com

Contact Ravelin

www.ravelin.com/contact-us




 290 Caldari Road,
Concord, Ontario L4K 4J4
Canada

--

 hello@merchantfraudjournal.com

 www.merchantfraudjournal.com

 1-(888) 225-2909