goTRG®

THOUGHT LEADERSHIP REPORT

Omnichannel Returns: Why Retailers Are Facing Record Fraud and How to Prevent It

Introduction

For every $100 in returns, retailers lose $10.30 to fraud[1]. Some instances occur from outright theft, while other fraudulent transactions are less nefarious—such as wardrobing[2]. As returns reach over $761 in lost sales annually, retailers must address the $78.4 billion elephant in the room.

We sat down with our in-house subject matter expert on fraud and loss prevention to discuss why fraud is rising, threats ahead of the holiday season, how to spot predators, and the best methods to prevent loss in an age of increasing fraud.

For every $100 in returns, retailers lose $10.30 to fraud.[1]

1 Source: https://nrf.com/research/customer-returns-retail-industry-2021#:~:text=For%20every%20%241%20billion%20sales,shoplifting%2C%20collusion%2C%20wardrobing%20and%20more

2 Source: https://www.gotrg.com/post/tips-trends-for-recognizing-returns-fraud-in-electronics

The Covid Factor

Organized retail crime (ORC) is at its highest level of all time[3]. ORC losses averaged $777,877 per $1 billion in sales in 2018, up 7% from 2017's previous record. ORC was rising before 2020, but the pandemic-fueled shift to online shopping has further exacerbated the problem.

Today, more than two-thirds of retailers said the pandemic increased their organization's overall risk, and 57% indicated a rise in ORC[4].

Beware this Holiday Season

The holidays are ripe for retail and returns fraud. An increased number of purchases means more occasions for bad actors and organized crime rings to target stores and customers through phishing emails and credit card fraud. They can also take advantage of curbside services where credit cards and IDs aren't required.

3 Source: https://nrf.com/research/2018-organized-retail-crime-survey
4 Source: https://nrf.com/research/national-retail-security-survey-2021

Top Omnichannel Fraud Strategies

Somewhat predictably, store shutdowns and stay-at-home orders at the start of the pandemic prompted criminals to shift their tactics and operate in new channels. However, many tactics have remained the same.

BOPIS Fraud

According to NRF's 2021 survey[5], 39% of retailers said multichannel sales like buy on line pick up in store (BOPIS) were the most significant source of increased fraud—up nearly 20% from the previous year.

~20%↑

Buy online pick up in store (BOPIS) fraud—up nearly 20% from the previous year.

It makes sense that criminals would capitalize on BOPIS programs because they can quickly complete a transaction without presenting a credit card or ID in some cases and drive away with an item they never paid for. In addition, BOPIS allows fraudsters to steal without entering the store or visiting the website.

Returning Used and Stolen Merchandise

Many fraudsters capitalize on omnichannel capabilities by stealing and selling across multiple channels, often with the same retailer. Another growing omnichannel retail fraud trend involves returning stolen merchandise without receipts and claiming the item was a gift or defective to get a store credit or cash back.

In some cases, fraudsters will receive a full refund without returning anything at all. For example, they'll say the product was broken or didn't function properly and then return a box of rocks that weighs about the same amount as the item in question. This is particularly common among electronics like TVs and smartphones. Unfortunately, retailers often miss these cases because they initiate online refunds based on tracking numbers before inspecting the contents of the box, or their software is not sophisticated enough to track the serial number of the original item and match it to what was returned.

5 Source: https://nrf.com/research/national-retail-security-survey-2021

At goTRG, we've seen and reported this scheme for years. Our software was designed to track these fraud rings and helped our retail clients put these criminals behind bars. However, as retailers focus on eCommerce sales offer flexible return policies, the problem will persist.

Smishing, Phishing, and Pharming Attacks

Smishing, phishing, and pharming may sound ridiculous, but everyone should be aware and vigilant. These terms describe serious and rampant threats to retailers and consumers. Smishing attempts to steal people's logins and financial data by sending text messages that trick them into clicking a link or sharing personal details. The attack takes its name from phishing schemes, which "fish" for an email response that leaves the victims vulnerable to theft. Both are damaging, but smishing messages arrive directly on the phone, making them much more effective at achieving their goal. According to a September 2021 study[6], smishing and phishing attacks have increased by almost 700% since the beginning of the year.

Pharming is another major issue, where online scammers manipulate a legitimate website's

~700%↑

Smishing and phising attacks have increased by almost 700% since the beginning of the year.

traffic to steal the private information of that site's customer. Essentially fraudsters create fake websites that mimic real ones and redirect users to provide personal information on that platform.

As a result, criminals gain access to bank accounts and credit card details, allowing them to make illegal purchases, fraudulent returns, or resell items to other thieves on the dark web. In addition, some people use stolen information to buy gift cards, which they use to purchase items and sell them for cash.

Chargeback Fraud

Chargeback fraud, also known as friendly fraud, is widespread in eCommerce purchases. A shopper will buy something online using their credit card. Once they receive the order, they will dispute the charge with their card provider, claiming they never received the item or didn't personally authorize the purchase. According to a recent report from digital trust & safety

6 Source: https://www.itpro.com/security/scams/360873/smishing-attacks-increase-700-percent-2021

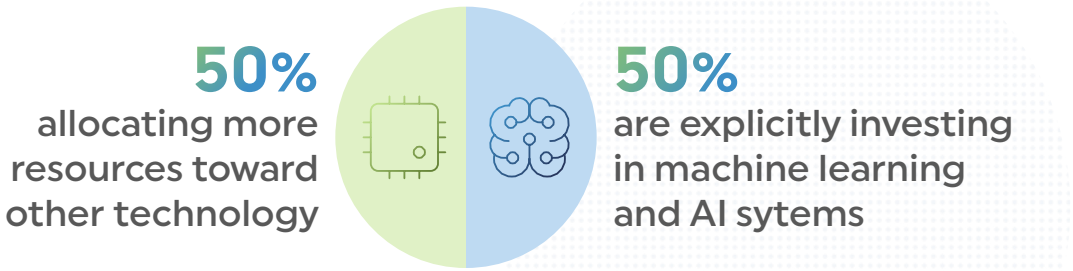
company Sift and their network of 34,000 eCommerce websites,[7] average daily chargeback claims increased by 19% from 2020 to 2021, and the average amount increased by 21% to about $293 per claim.

Sift also surveyed 1,000 consumers to determine the extent of the issue. The report found that nearly one in five has committed friendly fraud. In addition, one in ten consumers admitted to chargeback fraud to get money back on their holiday purchases.

What Retailers Can Do to Stop the Loss

eCommerce fraud surpassed $20B in 2021, an 18%[8] jump from the year before. As a result, retailers can no longer consider this loss a cost of doing business—retailers must take significant preventative measures.

For years, major retailers have been utilizing technology to detect purchase and return fraud, but now they're stepping up their games. An NRF survey[9] indicated half of all retailers are allocating more resources toward other technology while another 50% are explicitly investing in machine learning and AI systems for loss prevention.



Source: National Retail Federation, National Retail Security Survey 2021, Aug 17, 2021.

Retailers can minimize retail fraud by investing in top-level identification software, allowing them to verify customers' identities and implement "red flag" alerts for suspicious activity like inconsistent billing and shipping information. Advanced POS systems are the first line of defense for both online and in-store purchases.

7 Source: https://www.globenewswire.com/news-release/2021/12/15/2352951/0/en/Report-Consumers-Admit-to-Submitting-False-Fraud-Disputes-to-Get-Their-Money-Back.html

8 Source: https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report?utm_source=juniperpr&utm_campaign=pr1_onlinepaymentfraud_financial_fintech_apr21&utm_medium=email

9 Source: https://nrf.com/research/national-retail-security-survey-2021

Strong Returns Policy

Return policies are possibly the most significant determining factor for how much fraud a retailer may be exposed to. Organizations that offer lenient terms become vulnerable to fraud opportunities. Of course, convenient returns policies are also essential to inspiring more purchases, but retailers are starting to realize they can create stricter rules without sacrificing consumer loyalty.

Simple requirements should entail:

- Only accepting returns with a receipt, ID, and matching payment method
- Ensuring that all tags are intact and inspecting the item before issuing a refund
- Only processing refunds using the original payment
- Setting a deadline for returns between 30 and 90 days
- Monitoring customers that engage in excessive returns behavior and restricting their future purchases

Hire Right, Train Well

Employees are critical to preventing in-store purchase and returns fraud for multiple reasons. For one, honest, well-trained employees can look for warning signs and alert management or the loss prevention team when they see suspicious behavior. Conversely, dishonest employees can exacerbate the problem by issuing false refunds, skimming off the top, and giving away merchandise to friends and family. Retailers can run background checks before hiring new employees as a line of defense to determine quality talent.

Store associates must also receive training on loss prevention to spot common signs of fraud. For example, hesitation when providing personal information can be a tell-tale sign of a scam. Additionally, rush purchases and random orders can indicate fraud. According to Visa's guidelines[10], customers who don't seem to care what color or style they get and buy in bulk may be using stolen payment information with plans to resell those items online.

Strong Record-Keeping

One of the best methods to combat chargeback fraud is to keep immaculate records. So, when a customer initiates a claim, retailers must have proof to verify the transaction was real. Documents include POS records, signatures, credit card verification, IP address information, and delivery validation.

Retailers can also implement systems to prevent chargebacks by verifying higher than average transactions, flagging unusual activity like the billing address being too far from the shipping address, and verifying the customer's billing address before processing the transaction.

The Bottom Line

COVID-19 has significantly impacted retailers' risk landscape, making fraud an even more significant threat during the post-holiday returns season and throughout the year. Advanced monitoring technology is a highly effective strategy, but omnichannel retailers must also consider a multipronged approach that includes stricter returns policies and enhanced employee training.

10 Source: https://usa.visa.com/support/small-business/fraud-protection.html