

# Prepping for the Holidays

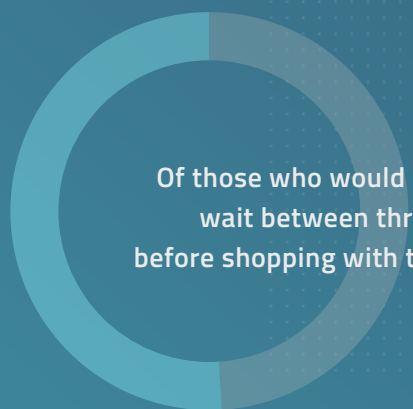
---

Balancing the Risks of Retail Fraud  
and Seamless Digital Shopping

In 2016,  
digital retailers  
lost nearly  
\$7 billion to  
fraud-related  
chargebacks.



Almost one-fifth (19%) of respondents said they would not shop again with a retailer if their personal information was hacked.



Of those who would return, 51% would wait between three and 12 months before shopping with that retailer again.

Along with the gift of increased online shopping, the holiday season also brings a big lump of coal: an increase in fraud. According to data from the **Forter Fraud Attack Index**, rates overall rose 13% in 2017, with activity spiking once holiday shopping began.

That's because enterprising fraudsters are as busy as Santa's elves, operating unseen in the avalanche of legitimate shoppers. And their malicious acts have significant bottom-line impact.

Research [found](#) that digital retailers lost nearly \$7 billion to fraud-related chargebacks in 2016. And if your customers fall victim to fraud on your watch, sales will suffer. Almost one-fifth (19%) of respondents in a [KPMG survey](#) said they would not shop again with a retailer if their personal information was hacked. Of those who would return, 51% would wait between three and 12 months before shopping with that retailer again. Those lost sales can be difficult to recoup.

If you don't have a solution that scales, you may be overburdened and let fraudsters slip through the cracks or decline genuine transactions out of fear.

# Popular Targets of Holiday Fraud

Here are the most common targets, in order of activity, according to Forter research:

1. **DIGITAL GOODS** like gift cards are among the top holiday gifts to give and receive, according to [research](#) from Deloitte. Malicious activity goes up during the final quarters as shoppers — and fraudsters — stock up. Forter found fraud for these items skyrocketed 167% last year.
2. **ELECTRONICS** are the top gift to receive, Deloitte found, and about one-third of the sector's annual sales are rung up between Thanksgiving and New Year's, Investopedia reported. Malicious activity in this sector rose 66% last year, according to Forter.
3. **FOOD AND BEVERAGE** sales increase during the holidays as people fill their pantries for celebrations and family gatherings. Fraud rates increased by 60% last year.

Two other verticals see higher sales — and fraud — volume during the final months of the year. Jewelry stores, for instance, do 28.6% of their sales during November and December, [according to](#) the National Retail Federation. Clothing is one of the top gifts, accounting for about 25% of shoppers' holiday budgets, per Deloitte.

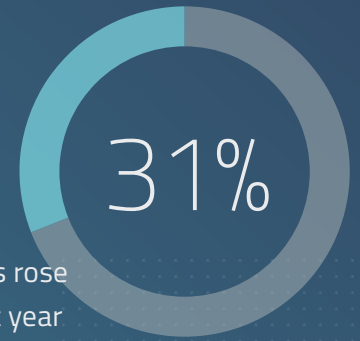
Malicious activity goes up during the final quarters as shoppers — and fraudsters — stock up.



# Common Types of Holiday Retail Fraud

Fraudsters make it their mission to find merchants' weak points along the customer journey. These scams are among the most frequent:

- **ACCOUNT TAKEOVER (ATO).** Fraudsters gain access to customers' account information using hacks or bots and start buying. Telltale signs include multiple failed login attempts, or logins from different devices or locations within the same network. Account takeovers rose by 31% in the past year, according to Forter, and Forrester [estimates](#) this crime creates up to \$7 billion in annual losses across all sectors.
- **DISCOUNT AND COUPON ABUSE.** Taking advantage of special discounts and coupons is an easy way to make money illegally. Look for repeated reuse of discount codes and similar email patterns, which indicate a fraudster is creating multiple emails to exploit referral discounts. The Coupon Information Corporation [estimates](#) this type of fraud "costs consumer product manufacturers hundreds of millions of dollars every year."
- **RETURN ABUSE.** Return abusers often return stolen merchandise or frequently return the same type of item. In 2017, Forter charted a 119% spike in return abuse directly following Cyber Monday. The [2017 National Retail Security Survey](#) from the National Retail Federation showed that return fraud was a growing concern for retailers in 2016, with an average cost (\$1,766) adding up to more than twice the shoplifting average (\$798). But return abuse is complicated. Retailers must beware not to block good customers from returning unwanted goods.



Account takeovers rose by 31% in the past year



ATO CREATES UP TO

\$7 billion in annual losses across all sectors



IN 2017, FORTER CHARTED

a 119% spike in return abuse

DIRECTLY FOLLOWING CYBER MONDAY



# 3

## FACTORS TO CONSIDER WHEN EVALUATING FRAUD DETECTION, PREVENTION AND PROTECTION SOLUTIONS

To protect your retail operations, you need a scalable fraud prevention solution that defends you and your customers even during the busiest shopping days of the year. Consider these three factors when assessing solutions for your store:

- 1. CUSTOMIZATION.** Each retailer has its own unique fraud pain points, so you need more than a one-size-fits-all solution. Choose a provider that can tailor and customize its system to your specific threats and scale.
- 2. AUTOMATION.** Advances in artificial intelligence and machine learning make automating the review process faster and more accurate than manual options. Look for a fully automated fraud solution that allows for real-time decisions, and check the service-level agreement to be sure the solution is actually real-time.
- 3. ACCURACY.** Speed is crucial in our on-demand digital world, but a quick erroneous decline isn't good for business. Investigate the accuracy rates of every solution you consider to ensure you only decline the fraudsters, not legitimate customers.

The right fraud prevention technology enables you to scale identification, as well as automate the approve/decline process in real-time with excellent accuracy.

- **TRANSACTIONAL FRAUD.** This crime is perpetrated across many site-based interactions. Check for inconsistencies in a user's information across a number of purchases, or questionable email addresses or phone numbers. Juniper Research [estimates](#) that online transaction fraud will reach \$25 billion by 2020.

When you prevent fraudulent activities in the first place, you reduce costly crimes, log a higher percentage of successful sales and cut chargebacks to your business.

## Fraud Prevention, Customer Experience and Loyalty

Holiday shoppers want you to protect them from fraud. About two-thirds of customers surveyed in the [Experian Global Fraud and Identity Report](#) said online security protocols make them feel protected, illustrating fraud prevention's role in customer satisfaction.

---

But you have to be careful not to add protections that produce another impetus for shopping cart abandonment (SCA) — a Barilliance study estimated the average SCA rate in 2017 was 78.65%.

Research published in *Procedia Computer Science* [found](#) that the higher the incidence of perceived risk to privacy and data, the higher the rate of SCA. That may be one reason why user account creation is a heavy motivator for SCA. One-quarter of consumers abandoned a transaction because too much data was requested, according to the Experian report.

And that's not the only way to lose customers early in the transaction. If your fraud prevention solution is too aggressive in declining transactions, many legitimate purchases and returns may be rejected. This can also insult loyal customers and prompt them to shop elsewhere. Many retailers already know they reject more transactions than necessary. What you may not know is that doing so doesn't just cost you a sale — the process could reduce the lifetime value of every customer who experiences it.

Similarly, manual fraud review bottlenecks delay order fulfillment. When holiday orders aren't delivered on time, you have the very real possibility of unhappy customers who are angry and embarrassed by missing gifts. If customers' children don't get their presents in time, those shoppers will never shop with you again.


---

All of this shows that consumers won't tolerate any added frustration in their purchasing experience, in large part because they have the option of shopping elsewhere.

In the end, retailers need to provide both convenience and security. A good fraud prevention system empowers you to add protections to and remove barriers from the checkout process, improving customer experience and eliminating friction.

Now is the time to start putting in place the protections necessary to prevent and detect holiday fraud. The last thing you need is to have your e-commerce site overwhelmed with traffic that your manual and technological fraud prevention solutions simply can't manage.

The best defense — for you and for your customers — is to get your fraud prevention solution in place now, ahead of the holiday season, and to ensure it runs efficiently and accurately in time for the holiday rush. You'll then be ready to safeguard everyone during the peak holiday shopping season and beyond.



In the end,  
retailers need  
to provide both  
convenience  
and security.

## About **F<sup>ORTER</sup>**

Forter is the leading e-commerce fraud prevention company that protects merchants during each stage of the customer lifecycle. The company's identity-based fraud prevention solution detects instances of fraud beyond transactions in real-time, such as attempts at account takeover and return abuse.

A team of world-class human analysts constantly update Forter's machine learning solutions with cutting-edge insights and research, ensuring the proprietary algorithms adapt to the latest fraud trends in real-time. As a result, Forter is trusted by Fortune 500 companies, online travel businesses, and fast-growing digital disrupters to deliver exceptional accuracy, a smoother user experience and elevated sales at a much lower cost.

---

Visit [www.forter.com](http://www.forter.com)