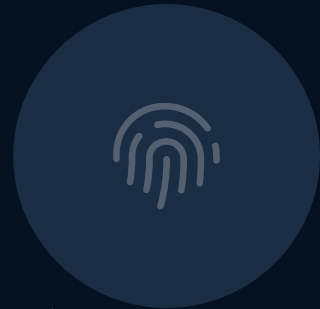




**Is My
Full Service Fraud
Prevention Solution
Effective?**



Contents

Chapter 1

Addressing eCommerce Fraud 3

Chapter 2

What Vulnerabilities Should Fraud Prevention be Addressing? 5

Chapter 3

Protection Against Chargebacks 6

Chapter 4

Preventing Friendly Fraud 7

Chapter 5

Improving Approval Rates 8

Chapter 6

Eliminating Manual Review 9

Chapter 7

Reducing Cart Abandonment 10

Chapter 8

Transparency in Decisions and Evaluating Results 11

1 Addressing eCommerce Fraud

Global payment fraud is on the rise and is predicted to cost merchants \$40.62 billion in losses by 2027. It is no wonder **the global fraud detection and prevention (FDP) market size is expected to grow from \$20.9 billion in 2020 to \$38.2 billion by 2025** (Markets and Markets, 2020).

This ebook will explore what merchants should expect from their full-service fraud prevention solution.



The ever-increasing rise in popularity of eCommerce enjoyed a sudden acceleration by the [recent pandemic](#) that forced many consumers to divert their spending from in-person to online. Whether or not they were ready for it, consumers and businesses alike were forced to shift their activities to a virtual arena hastily. Many consumers began transacting via new digital payments for the first time. The booming eCommerce market remains strong even as the economy reopened and a post-pandemic marketplace emerged.

The increase in eCommerce activity and the widespread use of digital payments have created even more opportunities for fraud. Retailers have come a long way from "Pay and Chase" fraud prevention, but so have fraudsters. As added security to in-person credit card use becomes increasingly sophisticated, criminals are turning their attention online and constantly inventing new ways to commit card-not-present (CNP) fraud, account takeovers, identity theft, and bot attacks—to name a few.

Enormous strides in technological advancements, such as smart bots that can optimize search for Google, are being used against eCommerce businesses by fraudsters seeking a payday. As potential payoffs increase and the cost of cyber attacks decreases, fraudsters are becoming more incentivized. The lack of aggressive prosecution for online payment fraud further emboldens fraudsters. According to [LexisNexis](#), **Successful monthly fraud attempts increased by 45% for mid-to-large retailers and 27% for smaller retailers.**



45%
of successful monthly
fraud attempts increased
for **mid-to-large retailers**








27%
of successful monthly
fraud attempts increased
for **smaller retailers**

2 What Vulnerabilities Should Fraud Prevention be Addressing?

ECommerce businesses must understand the actual cost of fraud and take appropriate measures to [mitigate fraud risk](#) and liability without stunting business growth. Employing fraud protection that is too rigid and doesn't account for fluidity in consumer behavior will block legitimate business and result in lost revenue. For example, many consumers have valid reasons for shipping items to an address that doesn't match their billing address such as, an extended vacation or working at a new job. Financial advisory firm, Aite Group, estimates that false positives could lead to eCommerce losses of [\\$443 billion by 2022](#).

The first step in establishing effective fraud prevention practices is identifying eCommerce vulnerabilities. Even if a business has not yet fallen victim to outright fraud, eventually being hit is unavoidable; it's just a matter of time. Additionally, there are hidden ways that fraud affects businesses.

The main culprits of fraud costing eCommerce businesses actual losses and missed revenue are:

-  Chargebacks
-  Friendly Fraud
-  False Declines
-  Manual Review
-  Cart Abandonment

3 Protection Against Chargebacks

Chargebacks occur when a customer disputes a charge with their financial institution. Often, chargebacks result from an unauthorized charge due to fraudulent activity. However, chargebacks can also result from merchant error, such as accidentally running a charge through twice or by a legitimate customer who is dissatisfied with the product or service.

Being hit with chargebacks is a telltale sign of inadequate fraud prevention. To prevent chargebacks, merchants need to become fraud experts. While many technologies are commercially available to merchants, such as fraud prevention built into eCommerce platforms or Address Verification Systems, being able to discern actual fraud from apparent fraud properly takes training and fundamental detective skills.

A full-service fraud prevention solution eliminates chargebacks by analyzing every transaction in real-time for signs of fraud. Algorithms can detect behavioral patterns and produce predictive analytics to protect customers from fraud and emerging threats with advanced technologies like machine learning, geolocation, and device recognition.

In addition to reducing, often eliminating, chargebacks, a full-service fraud prevention solution may offer a financial guarantee against chargebacks. If an order approved by the system results in a chargeback, the merchant will be reimbursed for the loss. Some tools, like NoFraud, also offer a **Chargeback Management service** that uses industry best practices to win chargeback disputes on behalf of customers.

4

Preventing Friendly Fraud

Friendly Fraud, which isn't very amicable at all, is carried out by legitimate customers seeking an easy refund. Typical claims involve fraudulent "Items not Received" or "Item not as Described" complaints.

To combat friendly fraud, merchants should take precautions, such as providing accurate item descriptions and images and utilizing trackable shipping options.

A full-service fraud prevention solution can further assist merchants in avoiding friendly fraud by tapping into proprietary data loops that track consumer behavior across regions and industries. NoFraud employs deep learning methods to continuously improve and adapt algorithms to keep merchants up to date with potential threats. Users can be notified of customers with a history of friendly fraud and can be blocklisted.

5

Improving Approval Rates

False Declines, otherwise called False Positives, are the rejection of legitimate customers due to suspicions of fraud. They are often the result of setting rigid risk rules or elementary fraud prevention thresholds.

According to research by Javelin, eCommerce businesses are often unaware that they lose 15% of their business to false declines. Legitimate shoppers who are declined simply opt to take their current and future business elsewhere and don't return to the site that declined them. Forter's annual eCommerce report for 2021 states that 40% of declined customers won't return following a decline.

In order to prevent fraud, many eCommerce businesses automatically reject high-risk orders, unaware of the number of good orders that are being discarded with the bad ones. A full-service solution employs an accurate decision engine and expert human analyst oversight to legitimize even high-risk orders.

6

Eliminating Manual Review

Manual Review is the time-consuming, tedious process of reviewing individual transactions for signs of fraud. Looking up shipping addresses, spending time on Google, and sometimes reaching out to customers in an attempt to verify their identity.

Many eCommerce businesses will manually review orders to mitigate fraud and false declines. However, manual review generally exceeds the purview of a typical merchant or employee, often diverting them from their primary tasks. Manual review also leads to fulfillment and shipping delays and is not a scalable solution.

Full-service fraud prevention can provide immediate 'decisions' for over 99.5% of transactions, not just 'scores.' This positive action eliminates manual review and relieves internal resources. If an order does require review, a team of expert analysts conduct the review and provide a decision.



7 Reducing Cart Abandonment

Cart Abandonment, or Checkout Abandonment, refers to unstarted or uncompleted checkouts. Shoppers may browse a site and put items in a shopping cart only to abandon the cart before or during checkout.

According to [Baymard Institute](#) research conducted on abandoned carts, 70% of shopping carts get abandoned. Sending cart abandonment emails is an effective way to [recover abandoned carts](#). However, being reactive is less effective than utilizing a [dynamic checkout tool](#). [Finance Online](#) estimates that \$260 billion of revenue lost to abandoned carts is recoverable by improving customers' checkout experiences.



70%

of shopping carts **get abandoned**



\$260 Billion

of revenue lost to abandoned carts is **recoverable by improving customers' checkout experiences**

8 Transparency in Decisions and Evaluating Results

Transparency from your fraud protection system is crucial in understanding and measuring fraud prevention performance. To understand what is going on, you need information on why orders are being canceled or approved and whether or not the solution was correct in rejecting specific orders. Here are some basic metrics to consider:

①

What is your Chargeback Rate?

The number of chargebacks you receive in a given period will indicate the level of fraud that your fraud prevention solution missed.

②

What is your Fraud Rate?

Your fraud rate is the number of fraudulent transactions canceled during the same period.

③

What is your Fraud Attempt Rate?

Your fraud attempt rate combines the chargebacks rate and the fraud rate. It will give you the total number of fraudulent transactions, those that got through and those that were blocked, that your business encountered.

④

What is your Approval Rate?

Your approval rate is the number of orders that your fraud prevention solution determined were legitimate.

⑤

What is your False Positive Rate?

Your false positive or false decline rate will indicate how much good business your fraud prevention is blocking.

Ideally, an eCommerce business would like an order approval rate of 99% or higher and a very low chargeback rate. However, the higher your fraud attempt rate is, the lower your order approval rate should be, indicating that your solution is successfully blocking fraud. Your false positive rate will primarily be based on your best estimate and customer feedback.

If, for any reason, you feel your order approval rate is not as high as it could be, consider reaching out to an alternative fraud prevention provider, many of whom, like NoFraud, will provide a free demo or trial so you can see for yourself whether or not your current solution is holding your company back by blocking too many good orders.

Conclusion

Full-service fraud prevention is suitable for any eCommerce business seeking to free up internal resources and increase approval rates and revenue. Allowing fraud experts to handle fraud eliminates fraud concerns and liability and increases ROI by unblocking false declines and reducing cart abandonment.

That being said, not all full service fraud prevention solutions are equal. If you are unsatisfied with your fraud protection software or are wondering if there is more that your fraud prevention solution could be doing for you, consider running a side by side comparison of your current solution and NoFraud. [Click here](#) for a free demo and see if you are leaving good money on the table.