NOFRAUD

The eCommerce Guide to Passing More Medium and High-Risk Orders

Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com

NOFRAUD

One of the most significant challenges online retailers face isn't losing money to fraudsters but losing money when legitimate customer transactions are incorrectly flagged as fraudulent and declined.

Multiple studies show false declines account for anywhere between 35-80% of rejected orders.

False declines, or false positives, can cause considerable damage to online businesses. Customers can become annoyed and embarrassed when they receive a notice of a declined transaction. And once falsely declined, as many as 39% of those shoppers choose to never return to that store again. Not only will these shoppers take their business elsewhere, but they'll tell more people about their negative experience than they would a positive experience.

A study by American Express found that customers tell an average of nine people about a positive shopping experience, while negative experiences are shared with an average of 16 people. These dissatisfied customers often express their displeasure to friends and family or in public channels like social media or review sites — sites you may not be monitoring that could be damaging your brand.

To prevent false declines and improve approval rates on legitimate orders that may be flagged as medium or high risk, we need to understand the risk spectrum and how it influences a fraud prevention solution.

The Risk Spectrum

In fraud prevention, different levels of risk are used to categorize transactions, behaviors, or activities based on their likelihood of being associated with fraudulent or suspicious activity. These risk levels help organizations prioritize their fraud prevention efforts and allocate resources effectively. The specific definitions and criteria for these risk levels may vary from one organization to another, but here are commonly used levels of risk in fraud prevention.

Low Risk

Low-risk transactions are those that have a low likelihood of being fraudulent. These transactions typically exhibit consistent and familiar patterns, and they often involve established and trusted customers. Low-risk transactions may undergo minimal scrutiny or intervention from fraud prevention systems and are generally safe, legitimate purchases.

Medium Risk

Medium-risk transactions fall between low and high risk. They may exhibit some irregularities or deviations from typical patterns but are not extreme or highly suspicious. Medium-risk transactions require moderate scrutiny and may trigger additional verification or monitoring.

High Risk

High-risk transactions have a significant likelihood of being associated with fraud or suspicious behavior. They often involve unusual or highly irregular patterns, large monetary values, an industry that sees a high rate of fraud, or other known fraudulent indicators. High-risk transactions require immediate attention, investigation, and intervention by fraud prevention systems or analysts.

Risk Categorization Considerations

It's important to note that the specific criteria and definitions for these risk levels can vary based on the industry and the fraud prevention systems and tools in use. Merchants often employ a combination of automated systems, machine learning algorithms, and human expertise to assign risk levels and respond to potentially fraudulent activity effectively.

Some businesses also use dynamic risk scoring models that continuously assess the risk of transactions and adjust the risk level based on real-time data and evolving fraud patterns. This helps maintain flexibility during risk assessment and helps to minimize false declines that might come when fraud filters are too rigid.

NOFRAUD

False Positives and the Over-Automation Problem

Most full-service fraud prevention solutions rely heavily on automation for decision-making. This means that their algorithm contains a threshold for the amount of risk that they are willing to tolerate.

Anything above that threshold will be automatically declined based on the risk score determined by the algorithm.

If the fraud provider uses a more conservative threshold, you get the benefit of rooting out more fraudulent orders. However, the downside is that you're almost certainly declining good customers as well.

Conservative Approach

- \+ Fewer Chargebacks
- − More false positives
- − Greater risk of poor customer experience

Conservative pass/fail threshold

Alternatively, an aggressive approach may allow more fraudulent orders through, but you benefit from fewer false positives.

Aggressive Approach

- − More chargebaks
- \+ Fewer false positives
- − Potential penalties from payment processor
- − Encourages more fraud attempts

Aggressive pass/fail threshold

Some fraud prevention companies offer the option to select different risk thresholds through a guaranteed approval rate for orders. This means that if you pay a higher percentage per transaction, the fraud prevention company will increase the approval rate by raising the risk threshold behind the scenes.

However, it is important to note that the rate you are charged is calculated carefully to avoid losses on behalf of the fraud company. Even though you are guaranteed a higher order approval rate, you will have to pay higher fees for it. This might encourage more fraud attempts, which could negatively impact your relationship with your payment processor.

NOFRAUD

Effects of Rigid Fraud Filters

Overly strict risk criteria can lead to false declines, which negatively impacts both merchants and customers. False declines occur when legitimate transactions are wrongly rejected due to an overly cautious or rigid fraud prevention system. Here are some of the consequences of unyielding risk criteria.

Legitimate Customers Get Denied

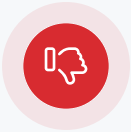
Strict risk criteria may flag perfectly legitimate transactions as high-risk due to minor discrepancies or unusual behavior. This can lead to loyal customers having their transactions declined, causing frustration and potentially driving them away.

Lost Revenue

False declines can result in lost sales and revenue for businesses. Customers who experience a declined transaction may abandon their purchase altogether or seek out a competitor with a more user-friendly payment process.

Customer Dissatisfaction

False declines create a poor customer experience. Customers encountering this issue may be less likely to return to the same merchant or recommend it to others.



Reputation Damage

Repeated false declines can damage a merchant's reputation. Customers who consistently experience difficulties with their payments may share their negative experiences online, harming the brand's image.

High Maintenance Costs

Depending on stringent rules alone to manage risk requires constantly monitoring and changing those rules as fraud trends, shopper behavior, and your business continually change. This adds unnecessary overhead costs to your team, without additional value, and will likely still result in false declines because of the inherent inflexibility of this approach.

NOFRAUD

Understanding the Most Common Causes of False Declines

If you're wondering whether or not your fraud filters are too rigid, these are typical transaction patterns of legitimate customers who may be declined if risk criteria are too stringent.

Travel Spending Patterns

Cardholders often don't inform their bank or credit union of travel plans, causing their purchase behavior to be flagged as unusual. When customers make purchases from locations significantly different from their usual geographic area, it can trigger fraud alerts. This is especially true for international travel.

Moreover, when travelers have trouble with payment, they may make multiple attempts to complete transactions. And as they're traveling, they'll make frequent transactions from different cities or countries within a short time frame. All of these actions taken during travel can be seen as unusual and suspicious, leading to more false declines.

Large Purchases

Shoppers make big-ticket purchases less often; and when they do, it can appear outside of their normal spending pattern. Payment processors and banks often employ fraud detection systems that flag large transactions as potentially high-risk. While these systems are essential for preventing fraud, they can occasionally result in legitimate transactions being declined.

Gifting

Shoppers often change the shipping information on multiple orders when sending out gifts. When customers make multiple order attempts in a short period, it can trigger velocity checks designed to detect potential fraud. This is because fraudsters often try multiple transactions in quick succession to exploit vulnerabilities. However, legitimate customers may place multiple gift orders during holiday seasons or special occasions.

IP & Billing Address Mismatch

Transactions made from locations that don't match the customer's billing address can trigger false declines, especially if the customer is traveling or using a VPN. A mismatch in IP address and billing address is also very common for business purchases as the shopper is completing the purchase for a business that can be located in a different country.

AVS Mismatch

When there is an AVS mismatch, it means that the address entered by the customer doesn't match the address on record with the credit card issuer. While AVS checks are designed to prevent fraud, mismatches often occur due to a typographical error or the address on file being outdated. If a customer accidentally enters the wrong billing address, even if it's a minor mistake, the payment processor may flag it as a potential fraudulent transaction and decline the payment.

Even worse, clunky checkout experiences can confuse shoppers. When merchants ask for the shipping address first, it can be unclear to the shopper where to input the billing information — which is commonly a tiny checkbox that is easily overlooked.

It's also important to note that some payment processors don't support P.O. Box addresses; so if a customer provides a P.O. Box as their billing address, it might result in a mismatch. And since AVS is primarily designed for U.S. addresses, it may be less effective for international transactions and can result in more frequent mismatches.

Billing & Shipping Address Mismatch

Having different billing and shipping addresses is not necessarily an indication of fraud. Many legitimate reasons exist for shipping to a different address, such as the recipient not being available during the day to accept a delivery, sending a gift to a friend or family member, or even using a workplace address for delivery.

Outdated Payment Information

In some cases, shoppers may not be aware that their card issuer has issued them a new card with updated details like a new expiration date or card number. When they attempt to use the old card details, it can lead to declines.

NOFRAUD

Striking a Balance: How to Minimize False Declines & Capture More Revenue

Striking a balance between accepting riskier orders and capturing more revenue is a critical challenge for eCommerce businesses. While you want to minimize fraud and protect your business, you also don't want to unnecessarily decline legitimate orders. Here are strategies to help you safely pass riskier orders while preserving the customer experience.

1 Don't over-rely on automation.

Flagging orders based solely on a single anomaly like an AVS mismatch has proven to be more of a revenue blocker than an effective fraud prevention tactic. To safeguard your shop while also capturing more revenue, be sure to consider all order characteristics to determine the accurate risk of the transaction. Too many merchants will have very stringent rules to block orders where the billing and shipping don't match or if the AVS is not a match, resulting in an increase in false positives and uncaptured revenue.

Additionally, it's important to regularly review and fine-tune risk criteria to adapt to evolving fraud tactics and changing shopper behavior. A fraud prevention platform isn't meant to be a static solution, but rather it's dynamic and built to evolve and adapt to new shopping — and fraud — landscapes.

2 Recalibrate velocity check triggers.

When customers make multiple order attempts in a short period, it can trigger velocity checks designed to detect potential fraud. This is because fraudsters often try multiple transactions in quick succession to exploit vulnerabilities. However, legitimate customers may place multiple gift orders during holiday seasons or special occasions.

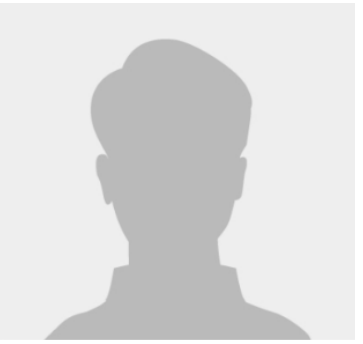
An effective fraud prevention solution can differentiate between genuine customers placing multiple gift orders and potential fraudsters. Work with your fraud prevention provider to implement more sophisticated fraud detection algorithms that analyze customer behavior over time which will help distinguish between these scenarios. The fraud prevention solution can set up customized fraud rules and thresholds that consider the unique characteristics of gift-related transactions. For example, they can set rules that allow for multiple shipping address changes within a single purchase session or adjust velocity thresholds during peak gift-giving seasons.

3 Implement a proactive review process.

Determining whether a transaction is trustworthy or not is usually quite straightforward. Most fraud detection software uses algorithms that analyze data from numerous sources and decide whether there are enough trust factors or risk factors to approve or decline an order.

However, the challenge arises when dealing with transactions that fall in the middle of the risk spectrum. These are transactions that do not display obvious indications of trustworthiness or fraudulence, or which may have signs of both. NoFraud refers to these transactions as "grey" orders, as they contain a high degree of uncertainty, with a significant number of both trust and risk indicators.

For example, let's say an order shows some suspicious signs: the address listed with the bank doesn't match the order, and the email used to place the order is brand new. These could be signs of a fraudster at work, or they could be signs of someone who just started a job in a different city making a purchase using their new company email.



Red Flags	Reality
Brand new email address	Got a new job across the country and just moved
Address Verification System (AVS) mismatch	Hasn't yet updated their address with the bank
IP geolocation different from billing address	Using their new work email to purchase supplies

Since this transaction also shows trust factors (CVV match, no risky device detected, etc.), it would likely fall under the category of a "grey" order. So without further review or verification steps, the determination of whether this order gets a pass or a fail is going to be dependent on your fraud prevention provider's risk tolerance.

Rather than over-relying on automation, all "grey" orders should automatically be escalated to a skilled review team — preferably one that is reviewing transactions 24/7. If you're using a solution like No Fraud, a proactive review team will also review select high-risk orders, such as orders with a very high order value, in order to capture more revenue.

In the example of the suspicious order above, a NoFraud expert fraud analyst would determine through additional research that the purchaser has started a new job at a company whose name matches the email used for the order. Alternatively, with your permission, they could request documentation to verify identity, giving the transaction a higher chance of being approved. In this case, after review, our analysts would pass the order that other fraud software would automatically decline.

4 Give shoppers the opportunity to correct typos before failing the transaction.

When customers modify shipping information or enter an incorrect address, it can trigger fraud detection systems to flag these transactions as potentially suspicious. This is because fraudsters may attempt to change shipping details to obscure their activities. However, legitimate customers may also need to update shipping addresses for genuine reasons, such as sending gifts to different recipients or updating an old address.

Maximize your approval rates by implementing a pre-gateway fraud prevention system that operates in conjunction with a dynamic checkout process. This checkout process will prompt customers to correct any typos or incorrect information in real-time, rather than screening orders post-gateway when it is too late to recover any orders that have been rejected.

5 Improve risk criteria by analyzing data from third-party sources.

Rejecting an order based on one or two factors is detrimental to business. It's important to regularly review and assess risk criteria as fraud attacks and shopping behaviors continue to evolve. The data on the order can tell you a lot but it helps to utilize other sources to obtain additional insight into each data point. By analyzing third-party data, merchants can use the additional insights to make more informed decisions about the legitimacy of transactions.

Beyond shipping and address verification or geolocation data, implement device fingerprinting solutions to analyze the device used to place the order. Compare device characteristics like IP address, browser type, or device type, with known patterns of legitimate customer behavior and known fraudulent activity. Be sure to incorporate third-party data sources into your fraud prevention solution's machine-learning models, so it so it can continuously learn from new data and adapt to emerging fraud trends — ultimately helping to improve predictive accuracy. The best fraud prevention providers are looking at thousands of data points — not a handful or even hundreds — in real-time to determine the legitimacy of a transaction.

NOFRAUD

Preventing Fraud and Preserving the Customer Experience

It's important to remember that the goal should be to maintain a strong fraud prevention system while ensuring that legitimate customers can complete their transactions without unnecessary disruptions. Striking the right balance can lead to improved customer satisfaction, increased revenue, and a positive reputation for the business. As you work to minimize false declines, be sure to keep these tips in mind:

- Regularly review and fine-tune their risk criteria to adapt to evolving fraud tactics and changing customer behavior.
- Implement multi-layered fraud prevention systems that incorporate various methods, such as behavioral analysis, machine learning, and manual review, to assess the legitimacy of transactions.
- Provide clear communication to customers about why a transaction was declined and offer a straightforward process for resolving the issue.
- Continuously monitor and analyze transaction data to identify trends and patterns, allowing for adjustments to risk criteria.
- Employ risk-based authentication that adjusts the level of scrutiny based on the perceived risk of a transaction.
- Rely on human discretion in cases where transactions are neither clearly legitimate or fraudulent.
- Lean on a fraud prevention solution that does all of the above and has the added bonus of screening a much higher volume of transactions and staying ahead of fraud trends.

NOFRAUD

About NoFraud

Founded in 2014, NoFraud is an eCommerce checkout and fraud prevention pioneer, ensuring every eCommerce merchant has access to the services and protection they need to scale with confidence. The company provides online merchants with costeffective, easy-to-use solutions that remove friction and fraud from their eCommerce funnel to grow sales and improve the purchase experience for customers.

NoFraud provides the industry's most accurate eCommerce fraud protection solutions to increase merchants' conversion and approval rates while virtually eliminating fraud. Visit www.nofraud.com for more information.

Ready to learn more?

Set up a trial with a fraud analyst and see how NoFraud will benefit your business, by approving more orders, relieving your internal teams from manual review, and having a positive impact on your bottom line.

✓ Start a Free 2-week Trial Today

Get in touch with a Fraud Expert. 888-773-3669 sales@nofraud.com nofraud.com