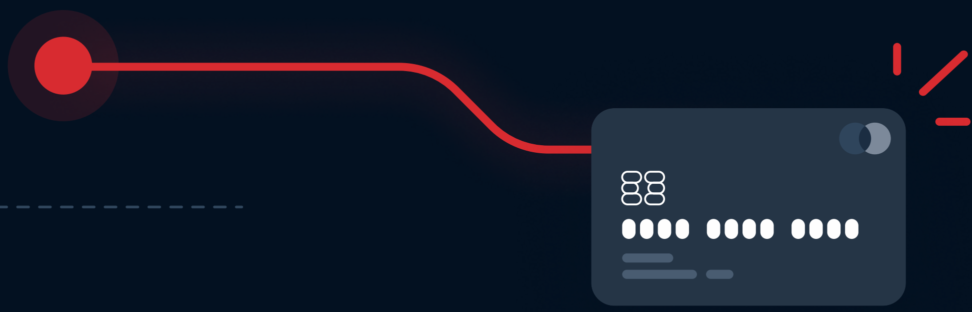

Avoiding Fraud False Declines

Maximize revenue by increasing approvals

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

Contents

1 What are false declines?

False declines, or false positives, occur when a merchant or a bank erroneously rejects a legitimate electronic transaction. Statistics show that, on average, 2.6% of all transactions are declined on suspicion of fraud. **A staggering 30% of these orders are considered false positives and should have been approved.** We've even helped some businesses reduce their number of declined orders by as much as 90%.

The state of eCommerce today is sobering. Some statistics:

~30%
of orders declined on fraud suspicion are **false positives**

69x
more losses from false positives compared to losses from actual fraud

>90%
of orders with an AVS mismatch are **good orders**

92%
of eCommerce vendors say "volume of false-positives" is **a key business challenge**

This eBook will examine some of the negative impacts of false declines, why they are so challenging to identify and mitigate, and what can ultimately be done to help reduce transaction rejections while increasing approvals and maximizing revenue.

2 The financial impact of false declines

The financial impact of false declines is great, yet it is vastly underestimated and misunderstood because they are tough to measure or quantify.

Lost revenue

The immediate impact of false positives is evident—when you reject an order, you don't realize the immediate revenue from that transaction.

Lost customer lifetime value

The immediate impact of false positives is evident—when you reject an order, you don't realize the immediate revenue from that transaction.

32% of respondents state that they would not shop again with a vendor where their card has been declined.

This figure might even be far higher when we consider that customers who experience any sort of friction in their shopping experience can easily go elsewhere.

Wasted Customer Acquisition Costs

False declines also render investments made in advertising and acquisitions wasted. It requires a lot of effort and spending to attract potential buyers to your site—an investment that is squandered when you simply end up rejecting those orders.

3 Common reasons for false declines

Difficulty tracking

The primary reason false declines are so challenging to avoid and root out is that most incorrectly declined customers never issue a complaint or offer feedback; they simply take their business elsewhere. This can be especially damaging in competitive markets where multiple vendors provide the same or comparable product. Even when you do hear customer complaints, it can be tough to tell whether or not those complaints are legitimate or whether a fraudster is cleverly attempting to social engineer your customer support team.

Incentivizing the wrong outcomes

Another critical reason that false declines are so commonplace is that vendors often incentivize incorrect outcomes. When CSRs are reprimanded for approving an order that ended in a chargeback and not recognized for decision accuracy as a whole, they are not motivated to approve orders that show any signs of risk, even if they might be legitimate.

Not getting the complete picture

Many companies neglect to consider the orders that are auto-declined directly at the payment gateway. A typical example of a gateway filter automatically declining transactions with an AVS mismatch--when a credit card billing address does not match a shipping address.

Frequently, there are legitimate reasons that shoppers make this mistake. One example is college students, who may live in one location while in school and thus, ship their items there, but handle their banking from a home address. If they are an international student, this might even be in another country. Up to 92% of all transactions rejected due to an AVS mismatch are suspected to have been safe to ship. Think of the lost revenue from that sobering statistic!

Clearly, you vastly underestimate your false declines if you do not include orders declined by gateway filters in your overall Order Approval rate.

Limited resources

Finally, limited resources will often account for elevated rates of declines that ought to be approved. This becomes especially problematic during the holiday seasons or periods of high sales volume when staff is experiencing heightened pressure and are overworked and fatigued.

4 Practical steps to reduce false declines

Now that we understand false declines and why they are so common, what can be done to limit rejections and maximize approvals?

Shift your mindset

Start from a position of assuming legitimacy. Instead of looking solely at risk factors, start looking at trust indicators to help you consider how the transaction may be legitimate. A mindset shift like this will help keep declines low and approvals high.

Here is a list of common trust indicators to keep an eye out for:

IP address

IP country and BIN match

Large Organizations (ex. "Wells Fargo")

Phone number

Not a burner

Carrier match between order device and phone number

Email credibility

Created a long time ago

Appears in online searches

Has been used frequently

Online behavior

Normal browsing behavior on website

Email domain

Organizational (academic, government, or legitimate business)

Match between country-specific email domain and device location

Positive history with other vendors

Have seen this customer before with similar behavior

In the case of the college student mentioned above, one data-checking technique would be to ascertain whether the shipping address is on or near a college campus or if the email address used has a .edu domain, which would connect the user with an institution of higher learning. Another excellent and timely example would be in the case of an employee using a corporate workstation. Their proxy usage might raise a red flag, but some searching will often yield evidence that the user is, in fact, legitimate.

Here's a list of some common scenarios of legitimate customers who may present red flags. This is why you can't solely rely on risk indicators and must instead consider the entire dataset holistically.

Scenario	Red flags you see
Using a corporate workstation	Proxy usage
College student	Billing/Shipping mismatch AVS mismatch BIN country and billing mismatch (international students)
Military personnel	Multiple location mismatches
International customers	Freight forwarder
Gifts	High velocity Multiple orders to different addresses
Furniture	AVS Mismatch Billing and Shipping distance

5 Don't just track passes and fails

Another great way to create a culture of greater awareness for in-house teams is to have your agents track their certainty level in their decisions. It's also helpful to examine your approval/rejection process and create a protocol for note-taking on why the CSR agent reached each decision.

Below is an example of how NoFraud tracks both positive factors and risk indicators evaluated and how that contributed to decision certainty.

Positive Factors

- Email address has been active for a substantial time frame
- Transaction placed with first payment attempt
- Issuing bank matches billing country
- Care Verification Value (CVV) match

Risk Indicators

- Risky device activity detected
- Address Verification System (AVS) complete mismatch
- Proxy detected
- IP geolocation is distant from billing address

Next Steps

- If you are uncertain whether your false-positive rates are too high, you are invited to consider a complimentary trial by NoFraud.
- By comparing the order approval rate of your current fraud solution to NoFraud's, you can identify whether or not this is an area where your business has room for improvement.
- Embrace your business' exciting potential by contacting NoFraud today for your free consultation and trial.

About NoFraud

NoFraud is an eCommerce fraud prevention solution that integrates directly with your eCommerce platform to stop fraud without turning away good customers.

We use a combination of powerful analytics, diversified data sources, and expert review to provide accurate pass/fail decisions in real-time with a financial guarantee against fraud-related chargebacks.