vesta

Addressing the False Decline Epidemic

WHITEPAPER

$130 Billion

This is how much CNP fraud will cost merchants between 2018 and 2023.

During the same time period, the ecommerce industry will spend $25.4 billion more on fraud detection and prevention technology.

Online merchants cannot be blamed if they built strong digital fortresses to protect their ecommerce businesses from fraudsters.

A recent survey by Experian reveals that 71% of merchants err on the side of fraud prevention versus the 29% of merchants who would try to approve as many legitimate orders as possible with the risk of having some fraudulent transactions go through.

When it comes to the impact on revenue, businesses look at the impact of both detection and permission-based security measures.

71%

Security measures err on side of detection (suspicion)

29%

Security measures err on the side of permission (trust)

What is your best guess as to the impact your security measures are having for preventing fraud? Security measures that err on the side of detection (suspicion) and probably declining more transactions than warranted based on incorrect assessments of these transactions as fraudulent when in fact they are legitimate? Or, security measures that err on the side of permission (trust) and are probably approving more transactions than warranted based on incorrect assessments of these transactions as legitimate when in fact they are fraudulent?

Image Source

67% of online merchants believe that undetected fraud is costlier than declining legitimate transactions. Only 33% believe otherwise.

The real billion-dollar question:

What's really costlier, undetected fraud or false declines?

The impact of false declines on your revenue

As it turns out, false declines are bigger profit leaks for online merchants than fraud itself.

Here's a simple calculation to back this up:

It's estimated that businesses lose **3%** of their revenue due to false declines.

In 2018, the ecommerce industry generated **$2.86 trillion**. If this revenue level stays the same until 2023, this would sum up to **$14.3 trillion**. At 3% leakage rate, false declines will cost the businesses **$429 billion**, while fraud will cost the industry $130 billion.

In short, false declines will cost merchants **3x more** than fraud itself.

More than meets the eye: other business impact of false positives

Money is the most obvious concern merchants have about false declines. However, there are other equally important damages false positives can inflict on businesses.

Here are the stats:

15%

A prevalent problem affecting millions of cardholders

At least 15% of all cardholders experience false declines with 1 in 6 cardholders being declined due to suspected fraud. Among those who are falsely declined, nearly 40% will abandon their cards, which leads to lost opportunities for merchants, banks, and card companies.

56%

Insulting the young generation of shoppers

One of the most affected customer segments when it comes to CNP false positives is the Millennials. Among the Millennials who are affected by false positives, 56% will stop purchasing from merchants that falsely declined their transactions. This is higher compared to the 39% of Gen Xers and 14% of Baby Boomers who will react the same way. It comes as no surprise that 42% of Millennials will do more transactions with merchants with fewer security hurdles.

5% to 40%

Turning the "big spenders"

Depending on their spending, online shoppers can experience a false decline rate of anywhere from 5% to 40%, and the number increases the bigger the value of their purchase is. Here are the decline rates based on customer spending: Less than $10 (5%); $10 - $24 (11%); $25 - $49 (5%); $50 - $99 (14%); $100 - $249 (26%); $250 or more (40%)

82%

Provoking negative reviews

Among those who get falsely declined, 82% feel embarrassed and aggravated. This can damage your online reputation as 92% of customers who experience a poor online shopping experience will write a negative review of the merchant.

Right under your nose: why false declines are under-reported or undetected

Why are many merchants finding it difficult to track false declines?

Too focused on fraud prevention

Businesses err on the side of suspicion and detection versus permission and trust

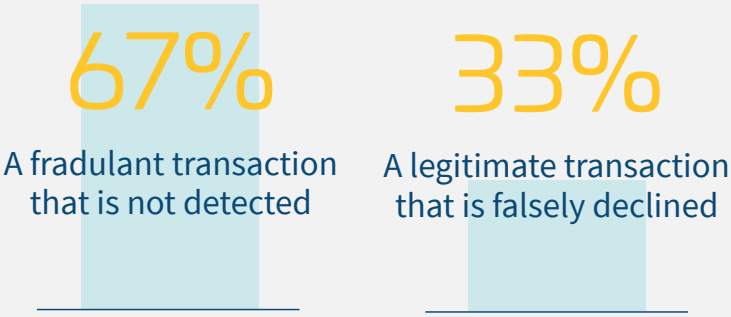

Image Source

While our calculations above showed that false declines are at least 3x costlier than fraud, the majority of businesses believe the opposite. 67% of businesses believe that non-detected fraudulent transactions are costlier than legitimate transactions that are falsely denied.

It comes as no surprise that a huge chunk of businesses' IT budget now goes to fraud-prevention solutions. It follows that with this investment, fraud teams are focused on preventing as many suspected fraud incidents as possible.

Lack of tracking mechanism

The market for fraud-prevention solutions and technologies is teeming with options. The same thing can't be said for false declines detection. Ideally, your fraud-prevention provider should provide a report on the number of false declines versus the number of prevented "real" frauds. Without this report, false positives are difficult to track, especially because it's rare for customers to report incidents of false declines directly to customer service.

A blindspot for false declines metrics

Aside from being too focused on fraud-prevention KPIs, many ecommerce teams can also have blinders, giving them tunnel vision to focus on sales metrics such as cart abandonment rate. False declines don't show in your Profit & Loss (P&L) statement. Therefore, without the conscious effort to track false declines, the problem can grow into a full-blown profit leak.

So, how do you diagnose a false decline problem? What are the metrics that you need to know?

How to diagnose a false decline problem

In order to reduce the number of false declines, you have to know your numbers. It is only through having an understanding of these insult metrics that you can put a reign on false declines before they become a business-threatening problem.

Approval rate vs. fraud detection rate

These two numbers should always be compared side by side because one can be indicative that there might be something in disarray with the other. An extremely high approval rate could mean that fraud incidents are not detected and prevented. On the flip side, a low approval rate can be an extremely high fraud detection rate that could mean a number of legitimate transactions are getting falsely declined.

Number of auto-declines

In 2019, merchants are expected to spend $25.47 billion more on fraud detection and prevention than they did in 2018. So, it's natural for merchants to assume that the transactions getting declined by their fraud prevention technology are accurate. It's rare for merchants to pay attention to the number of auto-declined orders and many remove these when calculating their overall approval rate.

However, the number of auto-declines can significantly impact the approval rate calculation. For instance, a merchant received $1 million worth of orders in a year. Out of these orders, $900,000 are auto-approved, $50,000 are auto-declined, and $50,000 needed further review. After manual review, the total approved orders came to $940,000.

Removing auto-declines from the equation, the approval rate for this merchant is 98.94%. Factoring in auto-declines, this will decrease to 94%. This almost 5% discrepancy is significant and even more so for merchants with a bigger total annual order value.

Decline rate at each stage of the payment chain

Knowing where false declines happen within the payment chain is important to pinpoint where a solution needs to be implemented.

False declines can happen at any of the following stages:

1. **Payment gateway.** Preset fraud filters run the first level of fraud checks on online orders.
2. **Third-party fraud protection system.** Fraud security vendors run additional security checks based on algorithms, machine learning, AI, risk database, etc.
3. **Bank approval.** The bank that issued the credit card runs additional security and authorization checks based on several factors. The bank either approves or declines the transaction.

Calculating your false decline rate

Finally, once you have identified the total number of false declines vis a vis the total number of orders, you can now calculate for your business' false decline rate. A 10% rate is a conservative estimate. Considering all the under-reporting, we estimate that the rate for most merchants is at 30%. It's very rare that we see merchants with a 0% false decline rate, which is indicative of an extremely loose fraud security system. So, the ideal false decline rate should be anywhere between 1% to 5%.

How to approve more legitimate orders

If after using these metrics you found out that you really don't have a false decline problem, kudos to you. That is really great news.

However, if you haven't done this exercise before, chances are you have a false decline problem. The severity may vary, but it should be addressed nonetheless—both to reduce your current rate and to make sure that your cybersecurity initiatives don't eat into your profits in the future.

Below are 5 ways on how you can prevent/minimize false declines.

1 Use customizable payment gateways

The preset filters of the current payment gateway you're using may be too strict, causing a significant number of orders to be falsely declined. Talk to your vendor regarding how you can tweak these filters to suit your business needs.

2 Choose a fraud prevention + acquiring solution with a proprietary risk database

Threats evolve. There are threats that affected online merchants in the past that are no longer relevant today. Choosing a fraud prevention solution that uses a proprietary risk database ensures that you are only declining orders based on current threats, thus increasing your approval rate. This database makes real-time decisions based on a fraud score which automates your first-level of fraud protection.

3 Increase manual review capability

Budget permitting, bolstering your manual review capability is an effective way to minimize and prevent false declines. You don't have to build an in-house team to do it for you. You can outsource this to a vendor that provides both automated and manual transactions screening. This may sound counterintuitive in an era of deep machine learning and automation. However, these automated tools need to be fed data to be effective and nothing replaces human interaction to get data from customers. With a bolstered manual review, you can directly get in touch with customers to verify their orders to increase your approval rate, as well as obtain additional data that can improve your automated false prevention strategies.

4 Give more leeway for high-risk orders

High-risk orders—above-average order value, high quantity orders, country of origin, etc.—are almost always automatically declined. However, these orders, while deviating from the norm, don't equate to fraudulent transactions. For example, if the order value is 5x the average, but the nationality of the customer matches the issuing country of the card used, the IP address matches the BIN of the card, and the billing address matches the shipping address, then the order is most likely legitimate. Using several data points does a lot better in painting the entire transaction story compared to cherry picking details that are outside the norm.

---

5 Tag approvals and declines

Again, the more data you obtain, the more equipped you will be in identifying fraudulent transactions versus legitimate orders that were falsely declined. Tagging the orders you declined and approved, and noting the reasons why you did, will allow you to identify patterns that you can use either to decline fraudulent orders that you previously approved, or approve legitimate orders that you previously falsely declined.

You don't have to stop business to stop fraud

At the end of the day, there will always be more legitimate online transactions than fraudulent ones. However, with headlines of fraud surfacing every day, no one can blame you if you want to protect your business from these cyber-thieves with a strong digital fortress.

Still, being able to prevent true fraud shouldn't be an excuse to ignore false declines, especially if it's your profitability and reputation on the line. It's getting more and more competitive out there and the customer experience is an important battleground among merchants to win and retain customers. False declines have become a part of that overall shopping experience. Ether merchants address this problem or suffer the consequences of losing their competitive edge and their customers.

Vesta Corporation is a pioneer in processing fully guaranteed Card Not Present (CNP) payment transactions for e-commerce merchants. We offer scalable protection payment solutions and patented fraud protection services. We focus on protecting your revenue from chargebacks and fraud so you can focus on your company's strategic growth.

Fight CNP fraud with no liability

Find out How

Get in Touch