riskified

3 Ways to boost your authorization rates (while still blocking out fraud)

Essential information payments executives need to know

PAYMENTS DIVE

Table of Contents

Introduction

Your company likely spends millions of dollars in advertising to entice consumers to shop with you. In the United States alone, digital advertising spending is expected to reach $298.4 billion in 2024. However, these efforts are wasted if customers walk away after a negative transaction experience on your online store.

Difficulty completing a purchase is a big reason customers give up.

Research shows that

67%

of retailers state that it's difficult to recover customers who experience failed payments.[1]

Customers will often blame payment failures on you, even if the problem lies somewhere else. "Merchants aren't always the ones making the determination to decline a transaction — it's the credit card issuer — and the consumer doesn't often know that," said Melanie Stout, head of recurring services at Optimized Payments. "All the consumer knows is that they were shopping online, their card payment failed, and they think that the merchant failed them."

A card decline can be embarrassing and insulting to the consumer, she added. It can feel like "the merchant is telling them they don't have enough money or credit, that they aren't good enough. That's how [payment failure] tends to reflect back on the ecommerce merchant."

[1] https://www.pymnts.com/study/fraud-management-false-declines-improved-profitability-ecommerce/

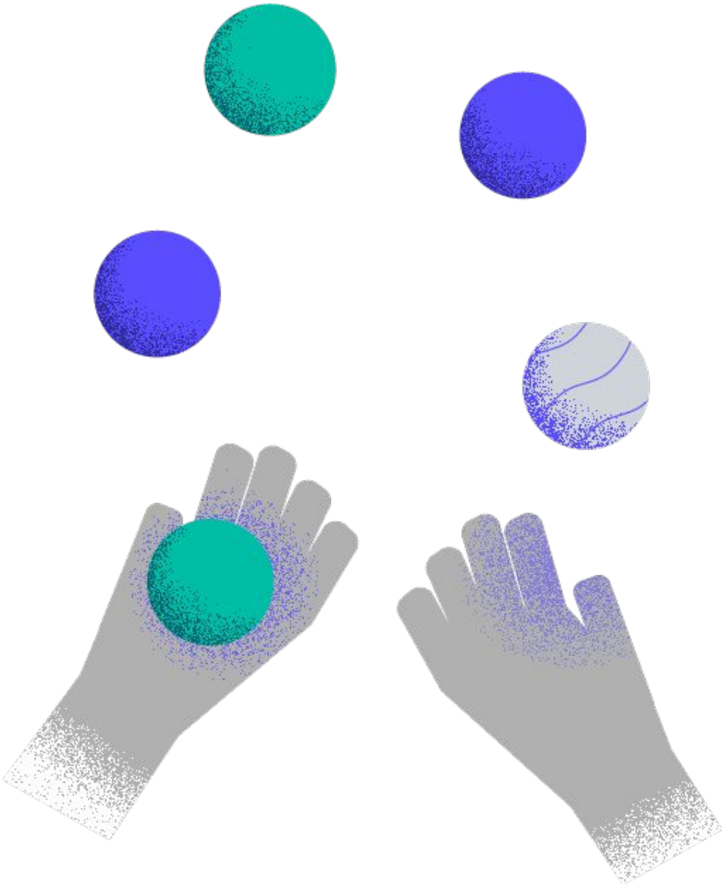
Approximately 15% of ecommerce orders fail because card issuers decline authorization, but up to 70% of those declined payments may be from legitimate customers, according to Riskified data.

What's worse: In the United States, merchants lose a whopping $157B a year to these false declines.[2]

How can you make sure you're not declining real payments and alienating legitimate customers?

It all starts with a holistic understanding of the payment process. After an online shopper clicks to purchase, the transaction goes through at least a couple of reviews. The **approval rate** refers to the percentage of orders that are processed after being submitted for fraud review. The **authorization rate** equals the percentage of transactions submitted to the card networks that are accepted.

This process might leave you feeling powerless when a third party makes the decision to approve a customer transaction. But this couldn't be further from the truth.



[2] https://www.pymnts.com/fraud-prevention/2023/only-a-third-of-ecommerce-merchants-know-if-fraud-caused-a-failed-payment/#:~:text=Latest%20data%20reveals%20that%20large,to%20false%20declines%20in%202023

01

3 common reasons low authorization rates happen (and how to raise them)

Declines occur for many reasons, and some of them stem from consumers themselves — such as insufficient funds or incorrect card information. But there are other reasons for low auth rates, and there are steps you can take to raise them.

Suspicion of fraud

“Payments fail for a variety of reasons, with **suspicion of fraud** being high on the list,” said Sudipto Chakravorti, head of product management with Fiserv. This is particularly true in industries like online retail and digital goods and travel services, which are more prone to fraud, he notes. “Issuers really tend to take a close look at those specific industry verticals before they decide to approve transactions.”

Work with a fraud partner to help you identify and stop more fraudulent charges before they reach the issuer. This will help issuers decrease the number of purchases they decline for fear of fraud.

History

Merchant-issuer history can knock auth rates as well. “If a merchant does not have robust fraud controls or has a history of higher chargebacks and fraud, all else being equal, that merchant is likely to have higher suspected fraud declines,” Chakravorti said.

Luckily, issuers themselves are doing more these days to improve auth rates and reduce false declines.

This is sweetening the merchant-issuer relationship. “It’s best for everyone in the ecosystem to get as much approval as possible, assuming the charges approved aren’t fraudulent.”

> “
>
> **Issuers are rolling out more and more machine learning, working with the big card companies to get more data and intelligence about what kinds of transactions are happening, and tailoring the risk scores.”**
>
> **Sudipto Chakravorti**, Head of product management with Fiserv

Siloed ecosystems

Another hurdle is a lack of data-sharing and communication between merchants and issuers. “I see **disjointed and siloed ecosystems** leading to higher authorization rate declines all the time,” said Chakravorti.

Issuers usually have a certain spec they want you to follow when reviewing an order, including relevant transaction details. “Even if the merchant could send more, they tend to send the bare minimum,” he said. While merchants may have access to data, gathering multiple data points from disparate data systems can require a lot more effort and reconciliation. This can lead to sending less data with a transaction in favor of speed and efficiency.

On the other hand, sharing more data about the transaction — customer details, deeper order-level data, and the like — can boost approvals. The issuer can analyze it along with the customer information they already have to make a better approval decision. In other words,

> “
>
> **It makes sense that if you overlay the two views — what the merchant knows and what the issuer knows — you will get a much more complete view.”**
>
> **Sudipto Chakravorti**, Head of product management with Fiserv

02

4 questions to ask a potential partner

Outsourcing some of these suggested solutions to risk management experts makes a lot of sense: Payments leaders have more on their plates than ever before. If you find the right partner, you'll see immediate results.

Essential questions you should ask:

01 Do you offer the flexibility of both pre- and post-authorization approaches?

One method to break through the silos that lead to more auth rate declines is to send as much data as you can before authorization. “That allows the issuer to send scores (related to) that customer’s profile back to the merchant,” said Chakravorti. This way, before you decide whether to approve or decline, you have additional information upfront about how the issuer feels about that customer. “Issuers have more information prior to the auth message,” he added, “and can adjust their tools to have a holistic view of that customer and the transaction and can also pass on better information.”

In general, more data at the pre-auth stage is a boost to decisions on both sides. “The other advantage of doing more work pre-auth is that opportunity for the merchant to identify card theft earlier,” said Chakravorti. “This goes a long way in terms of issuers red-flagging merchants who put through fraudulent charges.”

In some cases, you might prefer to keep a post-auth fraud review configuration For many stores, AVS (address verification) is an important risk signal, and this data point is available only after authorization. For merchants who build their workflows around a post-auth order review, working with a fraud provider that can add a pre-auth risk analysis gives the issuer confidence to authorize the payment.

02 Do you work with the newest technology?

Everyone talks about machine learning and AI these days, but not all machine learning is created equally, Chakravorti said. “Go deeper into the partner’s AI or machine-learning capabilities and find out what models they use. Is it a generic industry model used for all merchants in the industry, or is it more custom-developed?”

03 Is your decision-making rules- or models-based?

Rules-based tends to generate more false positives, Chakravorti said, so just having that as their go-to when dealing with fraud may cause an increase in false-positive declines.

04 Do their performance numbers speak for themselves?

Ask for verifiable numbers that demonstrate their performance with other merchants. That’s where the rubber meets the road. “Having a historical overview of what the partner has done with other clients is very important,” he said.

Risk intelligence provider Riskified is a publicly traded company whose performance metrics and finances are regularly audited. After partnering with Riskified, apparel retailer Lorna Jane saw a **54% decrease in cost of fraud and a 13% increase in authorization rates**.

Capital One’s integration with Riskified led to

25%

decrease in false declines with certain Riskified merchants

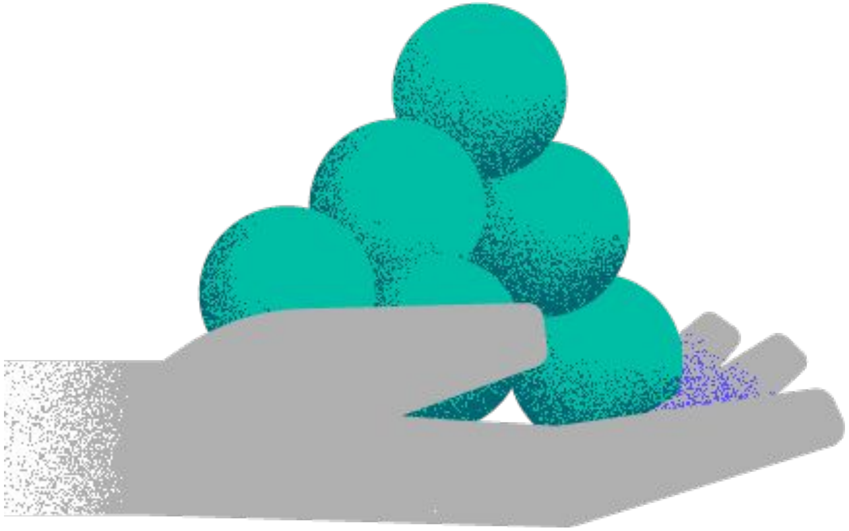
03

How your business benefits from higher authorization rates

We previously mentioned that 62% of customers whose payments were declined say they wouldn’t return to that online store. Realistically, the cost to your business is far greater.

“That number tells you that if a merchant wrongly declines a customer, it’s not only the loss of revenue for the merchant on that one transaction but on the potential revenue from that customer over time,” Chakravorti said. “Getting higher authorization approval rates helps with happier customers (and) higher ongoing revenue for merchants, and leads to less system disruption overall. In other words, the ecosystem itself is happier.”

In certain circumstances, improving auth rates can also erase unnecessary fees. If a customer’s subscription payment fails six months after the initial transaction, for instance, the merchant can retry the failed payment — but there’s a fee for each attempt, Stout said. “Increasing initial auth rates makes the flow frictionless for consumers while possibly decreasing fees down the line.”



Conclusion

Working with a vetted, accountable partner such as Riskified can improve your authorization rates and increase overall conversions. Riskified invests heavily in cutting-edge machine learning models to screen fraud with superior accuracy. Coupled with a chargeback guarantee, this gives the world's largest online merchants the confidence to unleash their ecommerce growth. You can rest assured that the threat and cost of fraud will be minimized, your merchant risk profile with issuers will be cleaner, orders will go through swiftly, and your customers will be far happier. Despite the fast-paced changes of today's market, one thing has and always will remain the same: Happy customers equal better business.

About Riskified

Riskified (NYSE:RSKD) empowers businesses to unleash ecommerce growth by outsmarting risk. Many of the world's biggest brands and publicly traded companies selling online rely on Riskified for guaranteed protection against chargebacks, to fight fraud and policy abuse at scale, and to improve customer retention. Developed and managed by the largest team of ecommerce risk analysts, data scientists and researchers, Riskified's AI-powered fraud and risk intelligence platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights. Riskified was named to CNBC's World's Top Fintech Companies in 2024.

For more information, visit Riskified.com or contact a chargebacks expert at hello@riskified.com.

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE