

# 7 WAYS TO BOOST PAYMENTS PERFORMANCE



# INTRODUCTION

So you want to improve your payment acceptance rates. First, we've got some digging to do. Payments can fail due to risk assessment, server-side issues and expired account details. At other times, it's a mismatch between data received and data expected. Yet many of these failed transactions can be rescued with some careful tinkering.

If you [understand the payment acceptance rate](#), you can apply strategies to recover revenue and lower your transaction processing costs. All of these add up to healthier trading profit.

This article considers the most effective strategies for increasing your payment acceptance rate. Namely, how to boost the proportion of attempted transactions that end in your business getting paid.



**Rémi Canard**  
Senior Product Manager,  
Checkout.com

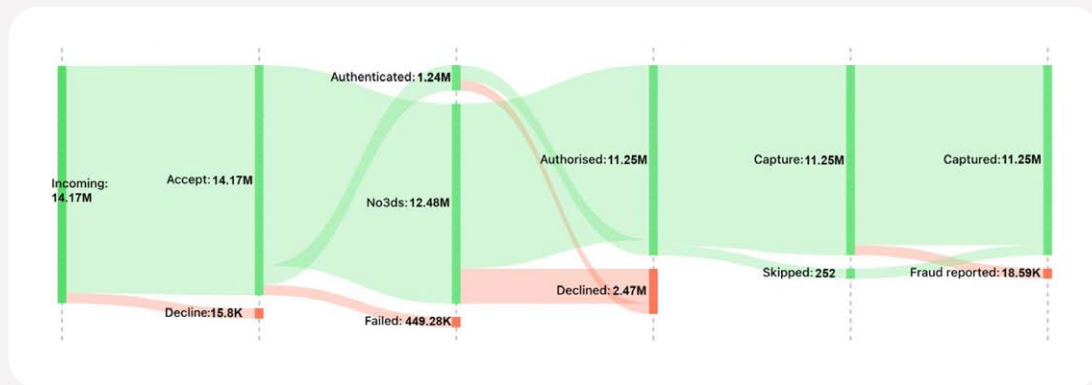
01

# IMPROVE DATA VISIBILITY

It can be difficult to trace the reasons for blocked payments due to a lack of visibility of [bank response codes](#) along the transaction chain. Additionally, issuing banks can also decide to decline payments when they lack the right level of supporting information. Compounding this, your processor could be making suboptimal routing choices without your knowledge.

Certain payment processing systems show you why your transactions are failing. Certain payment systems don't. For instance, the Checkout.com dashboard reveals the volume of your transactions dropping off at various stages.

## TRANSACTIONS



This chart shows the success and failure rates of total payments attempted for an ecommerce retailer. In the authentication stage, you will see that only 10% of online transactions are authenticated using 3DS, and a good chunk of those are declined at that point. It may be worth investigating the reasons so many payments fall at this hurdle.

Perhaps the fraud filters are working as they should, and your business is properly [guarded against ecommerce fraud](#). Or there may be certain [SCA exemptions](#) you can apply to these transactions to avoid authentication and capture a greater proportion of perfectly legitimate payment attempts.

02

# TWEAK PAYMENT MESSAGING CONFIGURATION

In an ideal world, we would have fund transfer systems with identical messaging preferences that automatically correct minor errors. Sadly, this world is not yet a reality. Instead, the financial standard for financial transactions – [ISO 8583](#) – is complex and while mandated, many differences of implementations can be found across the market. On top of this, the payments ecosystem is in constant flux, with regular updates that often deepen confusion. Therefore, we see [false declines](#) arise from payment messaging intricacies daily.

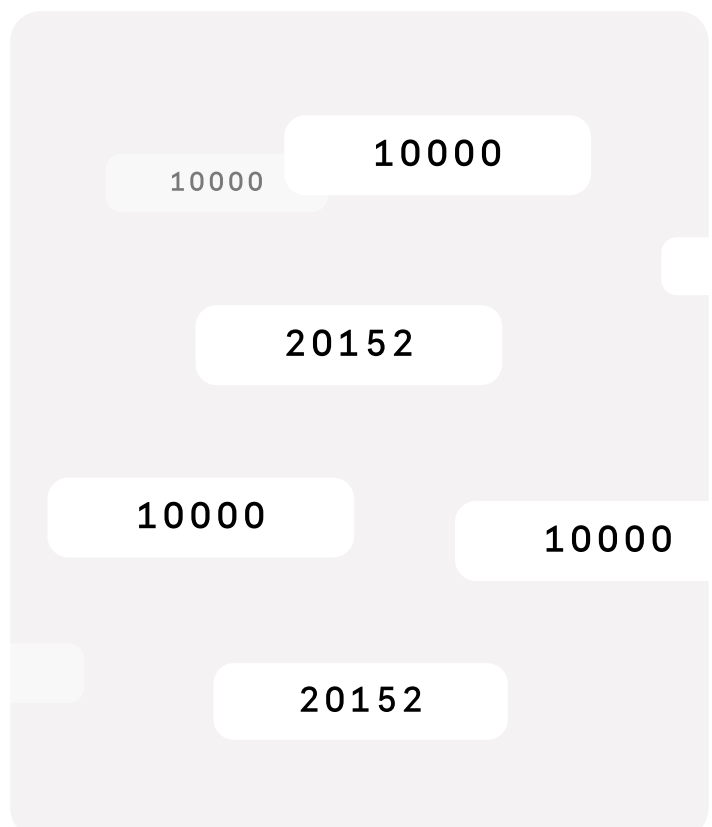
It's easy to let minor errors in payment messaging slip by unnoticed. But doing so can leave reams of revenue on the table. As any payment manager knows all too well, transaction processing can fail if just one field is incorrect.

To maximize payment success rates you need both correctly formatted data collection and high quality data. You must ensure each payment data field is correctly filled in, and payment messages are formatted appropriately.

## Example: Focus on payment ID

One app-based merchant at Checkout.com was including previous payment ID for customer-initiated transactions in outgoing payment messages. As previous payment ID is only ever sent for [merchant-initiated transactions \(MIT\)](#), the issuer falsely interpreted these as MIT and declined them.

A Checkout.com payments expert noticed this discrepancy and fixed the messaging error which led to an acceptance rate uplift for the merchant.



03

# AMEND PAYMENT DATA COLLECTION

Payments may be failing due to a shortfall in customer data collection. Certain cardholders may fail authentication because your payment gateway did not verify their IP address, for instance.

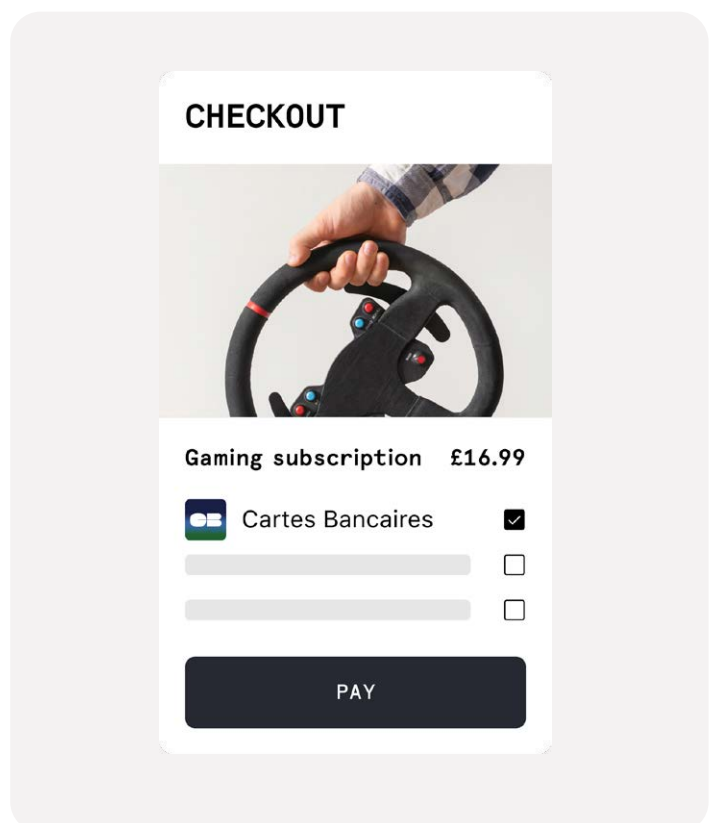
You should check whether your PSP has all the correct customer data needed for optimizing payment success. If not, then you may be able to gather extra data without much inconvenience to the cardholder.

Setting up [pull payments](#) can ensure smooth regular payment collections, and eliminate the need for customers to repeatedly provide data. So if your customer is logged into their shopping account on your app or website, much of their personal data (including billing address and phone number) is already available for collection. If traditional bank cards are not flexible enough in data requirements, consider connecting alternate payment methods such as PayPal or Apple Pay to ease friction.

## Example: The value of Localized payments expertise

“It can be a real challenge to identify local payment requirements in certain regions because they’re not written anywhere,” reasons Valeriia Chirkova, Technical Product Manager at Checkout.com. “That’s when you really need the access to vast datasets to spot patterns in declines.”

Chirkova’s team realized French card scheme Cartes Bancaires was rejecting some payment requests which didn’t include the customer’s billing address. Adding this – and other missing data points – achieved a 2% payment acceptance uplift for a gaming merchant in this market.



04

# OPTIMIZE AUTHENTICATION FLOWS

When it comes to authentication requirements, each issuer, card scheme and acquirer has its own unique preferences. For that reason, it can be hard to determine exactly which security protocol you should apply to each digital transaction.

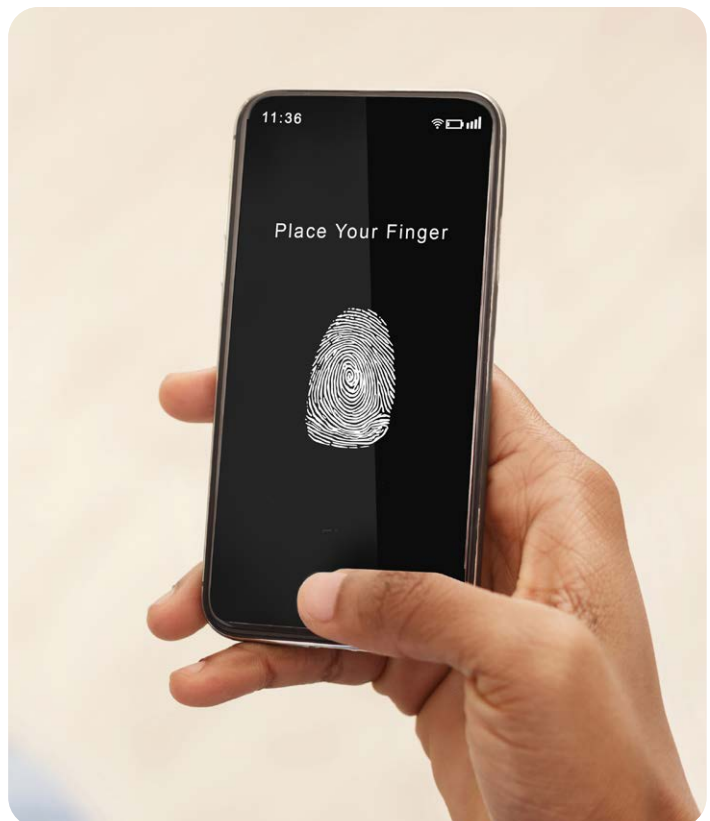
Often, it pays to look closely at patterns of declines for certain transaction types. When it comes to security measures, your payment processor may be doing too much – or too little.

For instance, European transactions are typically subject to Strong Customer Authentication (SCA), and will fail if these stringent standards are not met. However, many such payments can bypass SCA thanks to [exemptions](#). You can apply exemption messaging to certain payments to improve your authentication rate, thereby improving payment acceptance.

## Example: Re-routing based on exemptions

Your business has its own appetite for risk, too. And there could be revenue gains on the table if you had better knowledge of authentication protocols.

Checkout.com noticed a large proportion of a gaming merchant's payins were for small monetary amounts. That meant they were exempt from authentication according to SCA regulation. Applying the relevant exemption optimizations, Checkout.com secured a 9% boost in acceptance rate.



05

# ADJUST NETWORK TOKEN USE

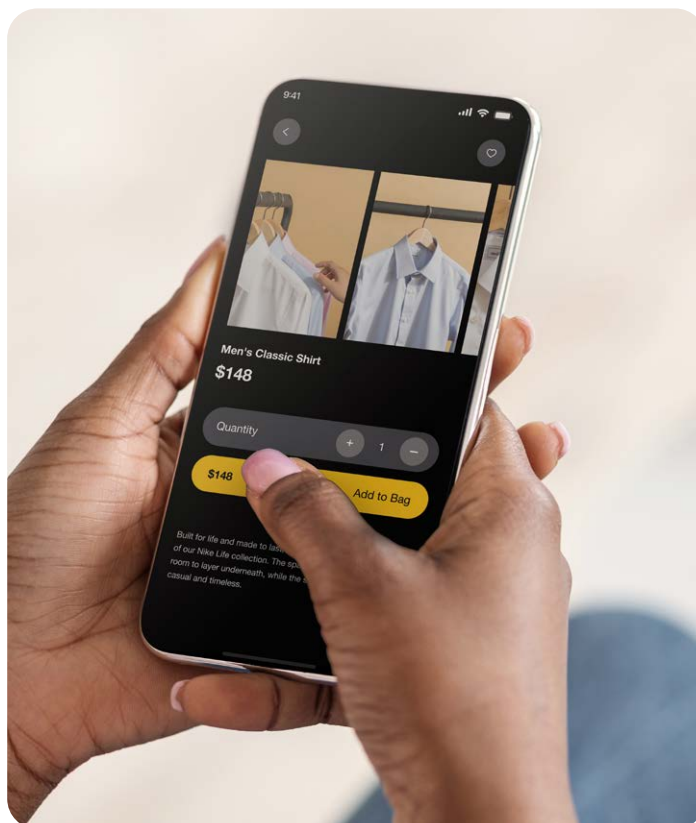
For some payments, an extra security layer is added that replaces the customer's card details with an encrypted token. The token [solves a lot of business problems](#), so it's a popular method of payment optimization.

Certain issuers expect tokens, and therefore tokenized payments are more likely to be accepted. Indeed, the payments industry as a whole is pushing towards token adoption; the Reserve Bank of India (RBI) banned ecommerce merchants and payment processors from [storing actual card data](#) as of January 1 2022, effectively mandating tokenization.

You could improve efficiency, security and acceptance rates if you correctly apply a tokenization strategy. While it's not as simple as "more tokenization = more revenue", careful consideration of which transactions to tokenize can increase credit card acceptance rates.

## Example: Introducing tokenization

Adding tokens into your payment ecosystem is a technically challenging process. For that reason, it can help to partner with your PSP account manager to make adjustments as needed. For example, one of our marketplace partners saw a 3% acceptance rate boost when Checkout.com designed their [tokenization strategy](#).



06

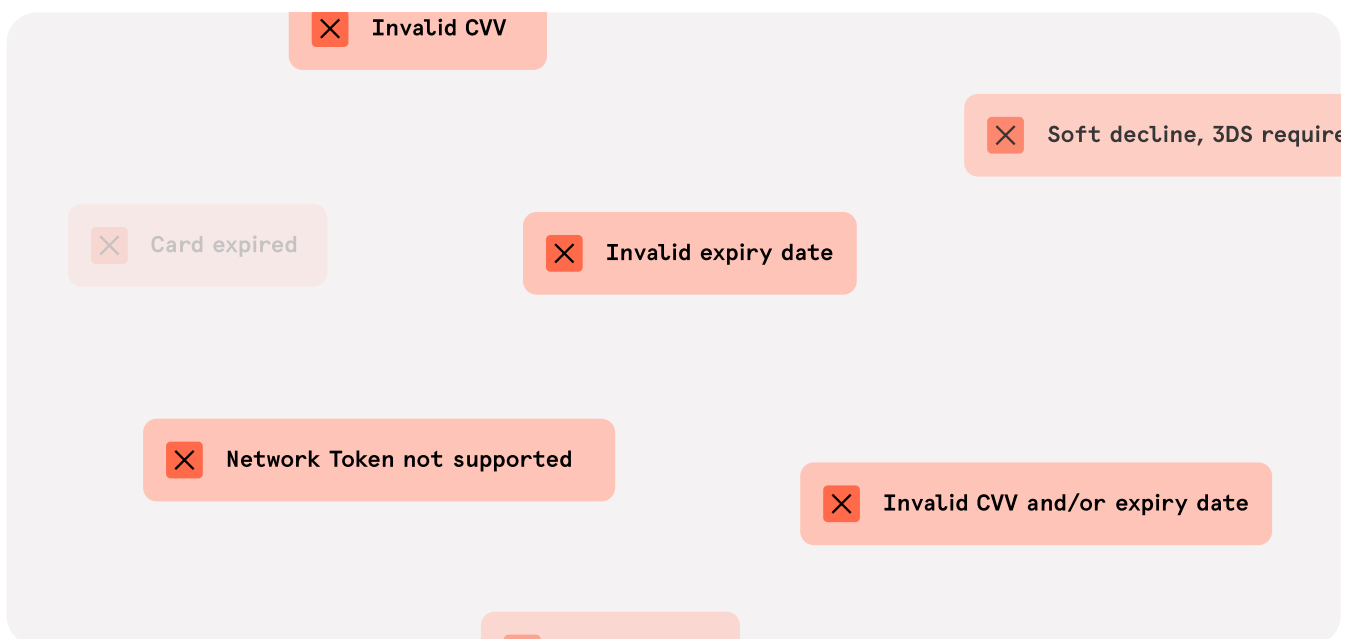
# REFINE YOUR RETRIES

You can retry payments that fail, either manually or using automated systems. It takes a fair amount of analysis to make the right call on which payments to retry and which to block.

For starters, it's critical to consider the [reason codes for declined payments](#). For instance, you shouldn't be retrying payments which are likely to be fraudulent. Remember, each retry costs your business, so it pays to be shrewd and only retry those with a high chance of success. Moreover, since April 2021, Visa has limited reattempts of a single payment to 15 times within a 30-day period.

Artificial intelligence tools such as the [Fraud Detection](#) analysis engine can support decision-making. It calculates a risk score for each payment based on billions of data points, so you can make more informed choices about how to route your payments. [Intelligent Acceptance](#) also has built-in retry logic (post-processing) to rescue otherwise lost revenue.

To measure success consider measuring the recovery rate: the number of transactions initially declined that ended up being authorized after retries. You'll need to factor in the total value of revenue from saved transactions versus the cost of the rerouting tools and analysis.





07

# UPDATE CARD-ON-FILE DETAILS

If you rely on revenue from repeat customers, you should pay attention to your [payment continuity strategy](#). A critical aspect of this is ensuring card-on-file details are valid before making a transaction request.

For instance, you could contact your customers by phone or email to ensure their payment details are up-to-date in time for their upcoming subscription renewal.

Or you could implement automation technology such as the [Real-Time Account Updater](#) to ensure customer payment details are renewed as soon as possible.



# HOW YOUR PSP CAN HELP YOU TO IMPROVE ACCEPTANCE RATES

There is a lot of technical detail involved at every stage of acceptance rate optimization. Suffice to say, there is no one-size-fits-all strategy to guarantee stronger revenue from your payment processing.

If you have strong in-house resources for payment analytics, you can begin by requesting transaction data from your PSP. If your business is not set up for this level of detailed payment investigation, you can engage your payments partner on a consultative basis.

## Requesting data from your PSP

It can help to get as granular as possible to discover where your acceptance rates are letting you down. Using backend analytics, you can isolate your acceptance rate data per the following:

Entity (i.e. each specific company)

Using Network Tokens (or not)

Issuer country

Issuer region

3DS challenge

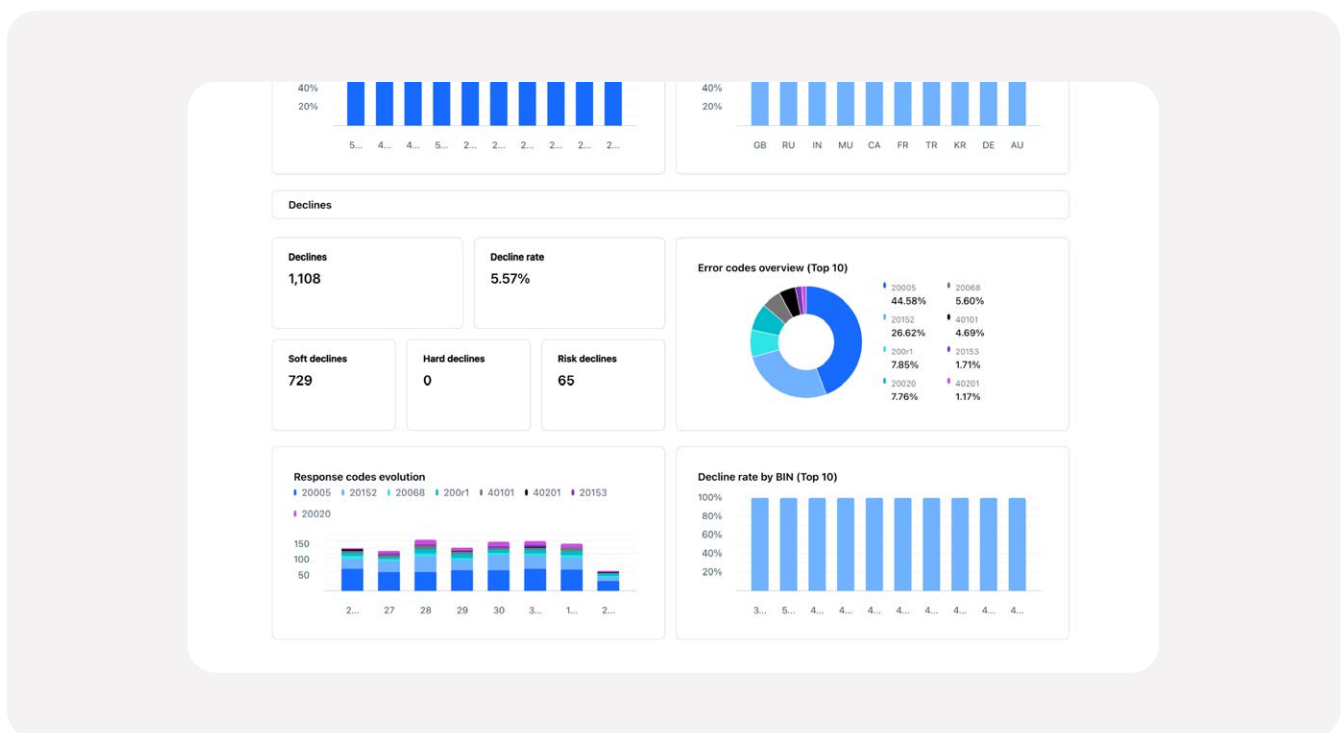
Other parameters are also available. You can request the data in real time or in a snapshot from certain dates. For instance, if you wanted to assess how well your optimizations worked over the peak season period, you could select the date parameters to view that breakdown.

If you want to analyze the reasons behind your failed payments, you can request the API response codes, save them in your own dashboard, and manually investigate the reasons behind each one. This will help you assess trends, and glean insights to inform your strategy adjustments.

It goes without saying that this approach requires a deep level of payment ecosystem expertise. The majority of our clients see success with a partnership approach: letting their payment service provider know their business goals, and allowing our success managers to carry out optimizations as needed. Machine learning tools such as Checkout.com's [Intelligent Acceptance](#) engine can automate these acceptance rate improvements.

Are you seeing the detailed data you need? Not all PSPs offer the same levels of insight into transaction success rates.

Here's a snapshot of the Data Explorer analytics dashboard from Checkout.com:



# HOW CHECKOUT.COM'S PAYMENT SUCCESS MANAGERS BOOST ACCEPTANCE RATES

As detailed above, we take great care to equip merchants with the data they need to maximize transaction success. In-market expertise, massive data networks, and sophisticated data processing tools equip us to continually improve your acceptance rates.

For instance, [Intelligent Acceptance](#) leverages Checkout.com's global data network and deep domain expertise to increase acceptance rates, lower transaction fees, and reduce operational complexity. It can also be leveraged with our Authentication, Network Tokens or Real-time Account Updater products to apply SCA exemptions only when necessary, or use the credentials that are most likely to increase acceptance.

On top of automated improvements, our success managers apply tailored interventions through account monitoring and the application of in-depth experience of financial technology.

Discover how [NordVPN](#) saw a 15% recovery rate on false declines thanks to improvements from Checkout.com.

