ACCEPTANCE RATE PLAYBOOK

checkout.com

INTRODUCTION

Looking at one figure in isolation isn't all that helpful. Say your acceptance rate is 85%. Or 54%.

Even 99%. Nobody can confidently declare which is the best for your business. There are simply too many complex factors at play; buyer behavior, scheme requirements, cyber-attacks, retries, conversion strategy, and countless other variables affect this figure.

The full revenue picture includes captures, approvals, and failed payments compared to total settlements – minus fees. You'll also need to take chargebacks and disputes into account.

Taking a multi-pronged approach to payment flow optimization is the smart way forward. One that takes account of all aspects of your transaction cycles. Only then can you diligently design a strategy for each locale, vertical, and customer type.

Indeed, optimizations can take place at any stage of the payment flow – which is why it's worth breaking down your strategy stage by stage. This guide is designed to help you do that.

This guide will focus on how we optimize success at four main stages of a transaction:

CHAPTER 1

AUTHENTICATION DECISIONS

Rémi Canard
Senior Product Manager, Intelligent Acceptance

CHAPTER 2

AUTHORIZATION ANALYSIS

Guillaume Merindol
Senior Engineering Director, Intelligent Acceptance

CHAPTER 3

REFINING RETRIES

Maxime Merabet
Principal Engineer, Retry Strategy

CHAPTER 4

FRAUD & DISPUTE FEEDBACK LOOP

Daniel Linder
Senior Director, Payment Performance

Alexia Le Tarnec
Product Manager, Disputes

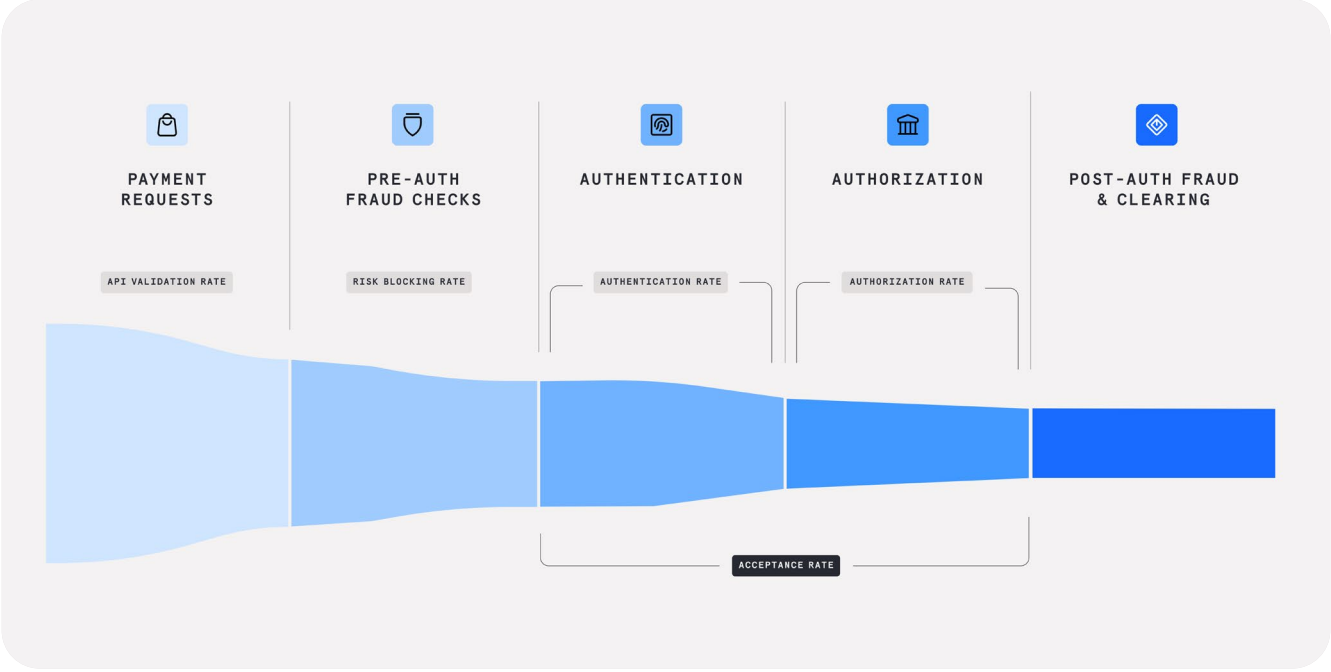
WHERE OPTIMIZATIONS TAKE PLACE

Our merchants trust us to manage their transaction cycles because they see improved revenue and reduced costs. Our payment processing algorithms are dynamic, meaning they update according to the latest card scheme mandates, regulatory requirements, and issuer preferences.

We optimize merchant transactions every day, with a dedicated task force to analyze each link in the chain.

That's why this guide contains many voices – we wanted to let each payment expert speak to their own area of specialization.

At Checkout.com, we calculate acceptance rate from the proportion of payments that pass through three stages: fraud risk assessment, authentication, and authorization.



Of course, post-authorization steps affect your acceptance rates, too, including your payment dispute management. That's why we included the final chapter on fraud and payment disputes, so you can analyze how and why to take these into account.

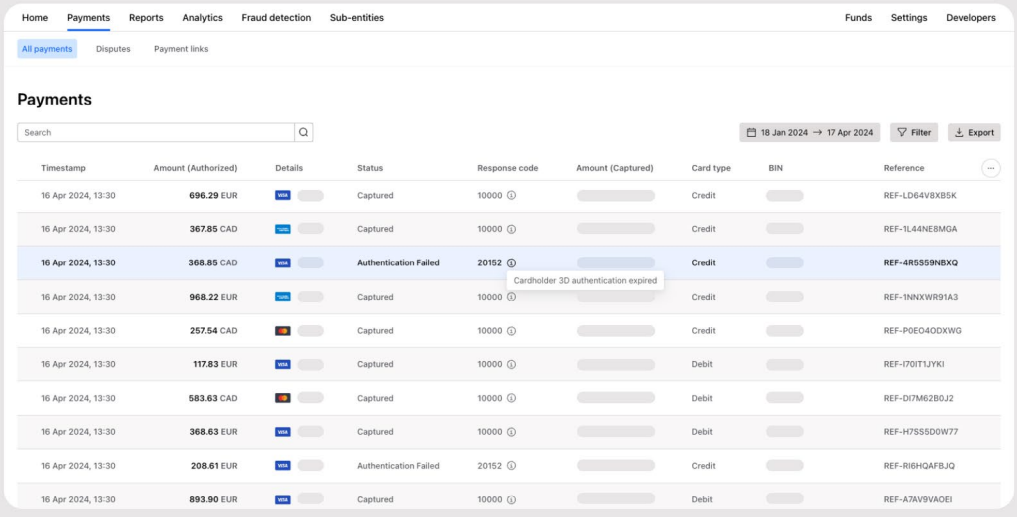
MORE DATA, FEWER PROBLEMS

Transactions can decline for a great many reasons. And as a merchant, you may be in the dark as to where and why your business payments are dropping off. Truth be told, smaller payment processors won't be able to decode your lower-than-desired acceptance rate. They just don't have the data.

Even if you could get some transaction data from your Payment Service Provider (PSP), would it be granular enough to offer useful insight? **When we surveyed merchants**, we found a worrying 45% of them didn't receive any actionable insights or analytics from their PSPs.

An end-to-end payment services provider has the capacity to retrieve, analyze, collate, and optimize your transaction. Combining software engineering with in-market expertise, Checkout.com has full access to data from the payment gateway, processor, and acquirer (plus authentication, fraud detection, and foreign currency exchange) because we own each phase.

We want you to own your payments success, too. This is why we offer better data visibility and greater customization than our competitors. In a world where **50% of merchants** don't receive response codes on failed payments, we clearly display your payments performance so you can maximize revenue.



Our advanced machine-learning products and experienced data analysts not only show you where and why your payments are failing but help you improve acceptance rates in line with your chosen strategy.

FACT-FINDING ON YOUR FAILED PAYMENTS

When you've invested heavily in your core product, marketing, and sales techniques, the payment technology aspect of your business can seem trivial. A customer that wants your product is going to persevere until they can pay for it.

RIGHT?

Well, payment friction matters more than you might think. **Our research found almost half (45%) of customers** won't retry payment after one false decline. Oxford Economics estimates that businesses lost between 1% and 2.1% of revenues (in 2022) due to inadequately optimized payments acceptance.

Imagine you had an in-store employee who refused to take payment from, say, two out of every hundred customers. Over time, your business is losing hundreds of thousands, if not millions, of dollars in net revenue. Negative effects of poor payment processing impact opportunities for repeat business, brand reputation, and customer loyalty. These knock-on effects can damage your market share, too.

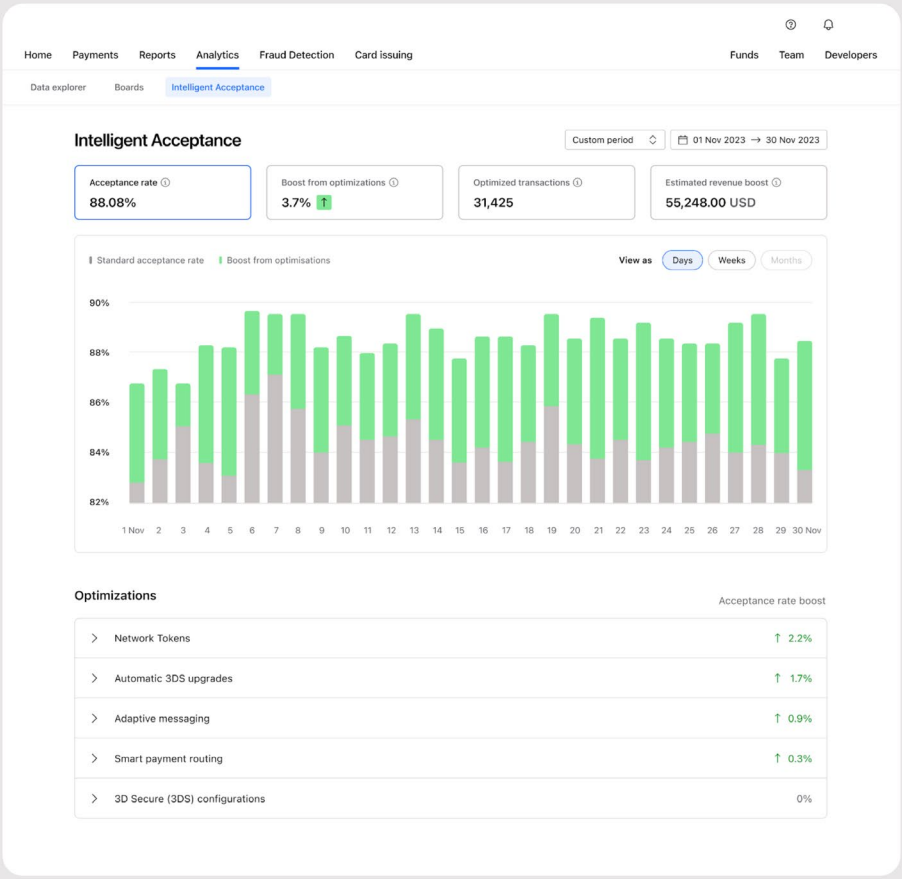
It's worth a conversation with that cashier to find out why they're rejecting payments. For a digital business, the equivalent is investigating your payment decline codes. Ultimately, you need to find out what can be done to address this revenue loss.

ENGINEERING PAYMENT OPTIMIZATIONS: INTELLIGENT ACCEPTANCE

You want your payments to succeed. So do we. At Checkout.com, we use machine learning to inform payment routing logic. Our decision-making engine, Intelligent Acceptance, makes customizable tweaks to your transaction payload so it has the best chance of reaching its intended destination. Our engineers test new optimizations and introduce improvements to the technology platform every week.

In this way, we react quickly to changes in protocol from issuers, card schemes, and regulators.

Transparency is vital for a successful collaboration with your payments partner. That's why we show you exactly what we're changing, and how it's affecting your payment success rate. You can see all this information in the Data Dashboard.



In the Data Dashboard, you can view the percentage difference between your baseline acceptance rate and the transaction success rate with individual optimizations applied. These are broken down by category, for example: 3DS configurations, adaptive messaging, Network Tokens, and smart payment routing. Within the Dashboard, you'll see recommendations to **improve your acceptance rate**.

The engine will make some personalized suggestions based on your live and historic payments traffic. However, the choice remains yours on exactly which adjustments to make.

By default, once Intelligent Acceptance is activated, all of your payment traffic will go through the system. However, you can choose to use Intelligent Acceptance in a smaller percentage for testing purposes until you feel comfortable applying the tool to all traffic. You can also choose to switch off certain optimizations such as CVV or AVS.

Next, we'll look more closely at optimizing payments at the authentication stage.

01

AUTHENTICATION DECISIONS

Rémi Canard
Senior Product Manager, Intelligent Acceptance

3DS DECISION-MAKING: IMPROVED CONVERSION BALANCED AGAINST RISK

Strong Customer Authentication (SCA) can reduce fraud, shift liability away from the merchant, and bring peace of mind for all parties. Of course, it's mandatory for transactions in certain regions, and issuers in the European Economic Area will reject requests that fail 3DS authentication. And we're seeing a push from Visa and Mastercard to require SCA in non-EEA countries such as the US, Australia and India.

The downside to SCA is the "friction" element of verification. While some payers don't mind this extra step, a proportion will struggle to complete it. Forgotten passcodes, problems with the authenticating device, issues with bank redirection, or the inability to biometrically authenticate can generate headwinds.

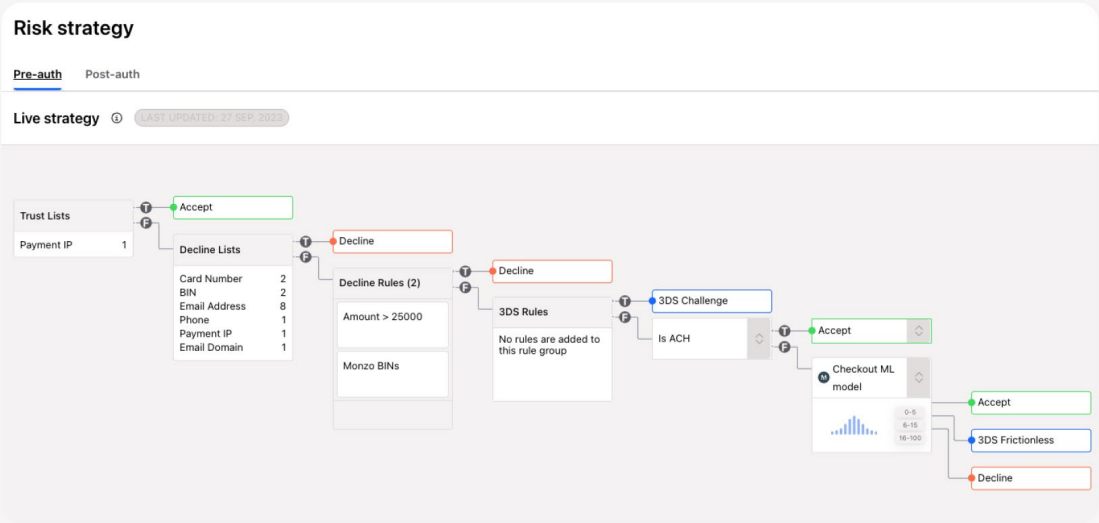
At scale, therefore, 3DS can damage conversion rates. In our research, we found **58%** of consumers were permanently put off from returning to a website or app due to an overly complex authentication process.

To mitigate this, our Intelligent Acceptance engine applies authentication exemptions such as **Transaction Risk Analysis** (TRA) and Low-Value Transaction (LVT).

We've seen acceptance rates improve up to 20% thanks to this adjustment. Our advanced machine learning engine analyzes each of your payment requests and automatically selects applicable exemptions. We also partner with schemes and issuers in order to mitigate the 3DS drop-offs as much as possible, using other forms of authentication.

Importantly, individual transactions are also risk-assessed, to ensure suspicious payments are sent via 3DS. This process is customizable according to your risk appetite, so you can keep control over the definition of "suspicious payments". Just one more way we improve conversion rates while maintaining high security standards.

Here is an example of a custom authentication risk management flow with Checkout.com:



You can add or remove rules according to your business preferences, in any desired combination, on parameters such as (but not limited to):

- Matching the payer IP to BIN
- Risk profile of the payer's country
- Address verification
- Card type or payment method
- Transaction amount
- Too many retries

DEVICE DATA COLLECTION AUTOMATES NO-CHALLENGE EXPERIENCE

Given the importance of conversion to your business, we develop our authentication products to reduce friction where possible. One way we do this is to instantaneously capture payer device data.

COMPLIANT PAYMENT PERFORMANCE

We want to be upfront about this: all of our payment processing technology ensures your business is fully compliant with financial industry requirements. It's vital for you to meet PCI DSS 4 standards at the authentication stage, so you need a PSP that gets you there. Not only do we meet PCI DSS standards, but also those of 3DS-PCI, EMVCo, GDPR, PSD2/3, card schemes, and other payment system partners. We can offer different modular solutions depending on your business's compliance needs.

Say, for example, you want to use **Authentication from Checkout.com** in the payment journey on your website or app. You can choose the integration type that best suits your business goals. Depending on your business's level of compliance, technical capability, and appetite for UX customization, you'll select the configuration that makes the most sense for your strategic goals.

Whichever integration you choose, our 3DS solution collects payer device data by default in order to assist with automatic authentication. For example, a payer who is using Apple Pay, who has authenticated their payment with a face or fingerprint scan, does not need to provide further authentication.

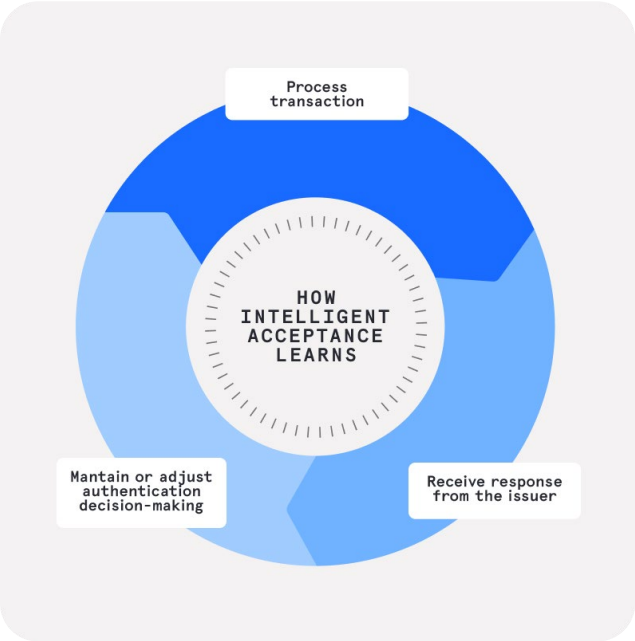
This means the payment experience feels quicker and easier for the payer, which can improve conversion. It's also good for boosting payment request approval rates, as many issuers favor transaction messaging with authentication data included.

Numerous studies find that the security of their payment details are a top concern for online buyers. Our latest research finds 83% of consumers would abandon their cart if they had concerns about the security of their payments data (n=8,000 Checkout.com and Oxford Economics).

Yet, security concerns must be carefully balanced with a low-stress payment experience for the user. So we won't require your customer to make any more effort than is strictly necessary to satisfy security and compliance needs. Our payment acceptance solutions allow you to adjust your payment strategy as desired, and pivot your authentication rules as your business needs evolve over time.

ADAPTING TO LOCAL ISSUER PREFERENCES

As a global payment processor, we're able to detect patterns in vast international data sets. Our machine learning algorithms improve authentication decision-making based on responses from individual global issuers. That allows Intelligent Acceptance to tailor your transaction traffic and match the authentication preferences of the relevant issuer.



Moreover, we continually update our algorithms in line with each new compliance mandate and local regulatory requirement (such as the SCA mandates in Australia). Intelligent Acceptance is structured to simplify payment routing for merchants. It integrates authentication decision-making that takes into account your global location and particular business preferences. So no matter where you are processing payments, they will be compliant with regional regulations, optimized for acceptance, and customized to your conversion strategy. Payments considered authenticated will be routed directly to authorization. We'll examine authorization more closely in the next chapter.

Fine-tune your authentication

Authentication is not a must-have for certain merchants, though it is a universally reliable way to cut fraud and improve issuer trust in your payment raffic. Adding another capability to the payment flow is almost always a good thing.

To keep more control over your authentication strategy, you can use a standalone solution such as **Authentication from Checkout.com** without enrolling in our full PSP product suite. That means you can take advantage of our sophisticated 3DS decision-making engine on your terms, with real-time steer over which portion of your traffic to route through it. making engine on your terms, with real-time steer over which portion of your traffic to route through it.

02

AUTHORIZATION ANALYSIS

Guillaume Merindol
Senior Engineering Director, Intelligent Acceptance

We know that **86% of merchants** do not have machine learning solutions from their Payment Service Provider (PSP) that help to reduce fraud or increase authorization rates. This needs to change. In an age of electronic money, our fine-tuned Intelligent Acceptance engine delivers tangible improvements in revenue, fraud risk reduction, and rewarding customer experiences.

Authorization has become a hyper-complex process, as the global digital payments ecosystem evolves with fractal-like intricacy. Even so, a major facet of boosting your acceptance rate is to laser-focus on issuer requirements. And we know you don't have all day and all night to decode those nuances. Nor could you even access all the relevant information to do so, unless you have direct relationships with all the issuers your customers use. As a full-stack PSP, Checkout.com bridges this gap.

While some PSPs take a "trust us, and we'll take care of it" approach, we're big believers in transparency and are eager to offer as much visibility into your payments performance as you need. In practice, this means round-the-clock access to data and analytics through the Checkout.com Data Dashboard, plus direct communication with our in-house payment experts to address ambiguous error codes.

Now that we've considered some best practices around authentication, we'll take a closer look at how to achieve transaction success at the authorization stage.

A DETAIL-RICH PAYLOAD

When it comes to the payment request, the quality of the payload has a significant impact on acceptance.

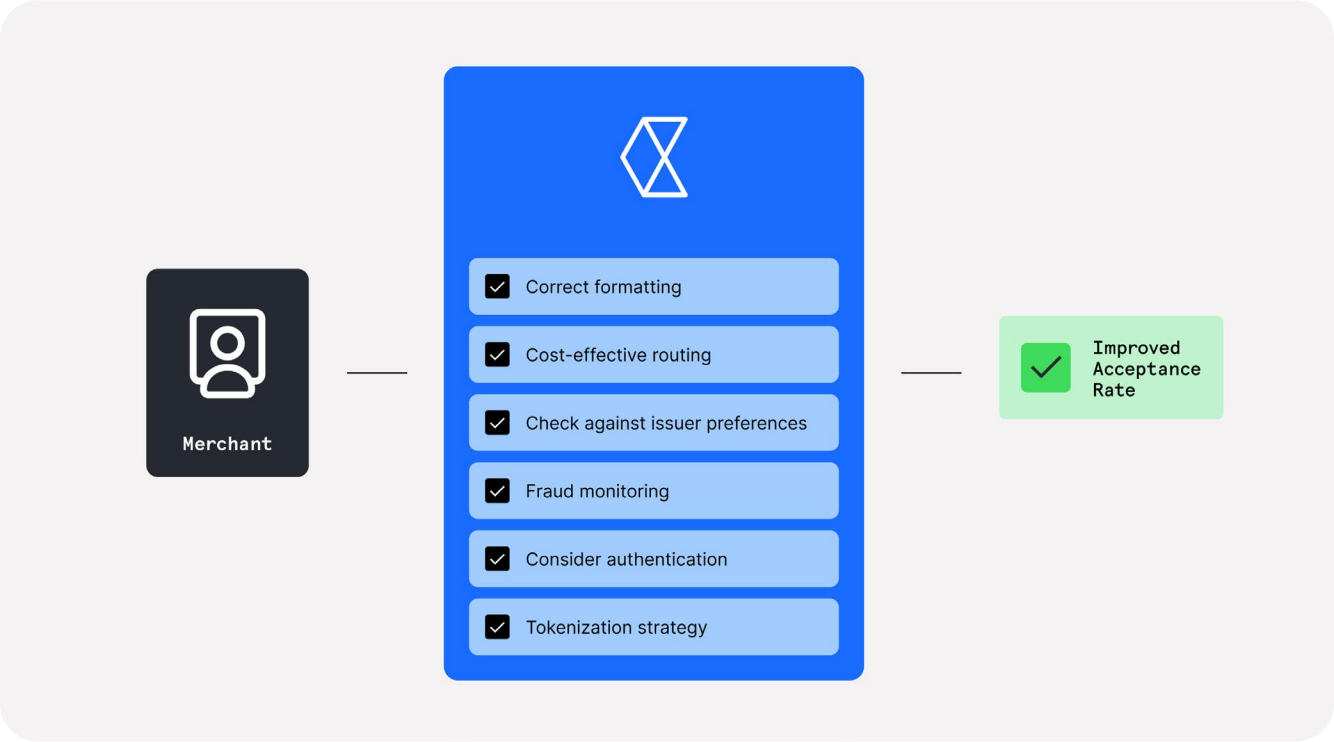
A golden rule is: if the payload includes extra data – be it the authentication, device data (such as IP address, device type, and a timestamp), and cardholder data (such as email address, delivery address, and billing address) – the more the better for authorization purposes.

Occasionally, merchants don't provide enough data for the payment processor to deliver transaction success. Granted, quite a few variables will affect the types of data needed in every instance. It's by no means obvious what to include or leave out. That's why we work directly with merchants to ensure we're on the same page and advise on the types of data we could use to help increase authorization rates. For example, an MIT needs to come with a previous transaction attached (as evidence of an initial authorization).

It's easy to forget this when you're wearing so many hats as a payments manager. We reach out to merchants who forget to include this and see their acceptance rate percentages improve as a result of sending along the extra data.

Of course we understand that buyer experience is critical for your business conversion, too. And the payer has every right to withhold consent for device data collection, and so on. That's why we prefer a collaborative approach with merchants. You know your business best, and we're here as your payments partners – not your payments boss. That means you always call the shots on which additional payload data to provide or withhold from us.

We suggest optimization techniques with a projected percentage of acceptance rate uplift, to help you weigh up whether or not the implementation would be a good business decision.



TECHNICAL IMPROVEMENTS AND CAREFUL DATA CONFIGURATION

Working with a wide array of merchants means we see a lot of mistakes in technical payment messaging. Schemes can release new mandates suddenly, leading to staggered issuer adoption. Our early adoption of scheme technologies puts us in a unique position to pick up on errors an individual merchant couldn't have foreseen. For instance, when the Reserve Bank of India mandated payment card tokenization in October 2022, we made sure our systems were ready for the change.

As a global payment processor, our oversight of billions of data points allows us to troubleshoot authorization failures better than an individual merchant ever could. But we're happy to help.

We bridge gaps in payment knowledge and repair poorly configured payloads before they reach the issuer. A simple example of this is reminding merchants that a subscription-based payment needs to include the ID of the original transaction (to prove it's authorized). Our in-house ID management solution can handle this for you.

Given the complexity of scheme and issuer requirements (not to mention regional regulations), it takes considerable expertise to identify and remedy payload messaging errors. Our Payment Success Managers personally monitor payment traffic to repair suboptimal formatting and submit missing details, as needed.

Cost-effective optimizations

We also take the time to save merchants from paying excess fees due to suboptimal payload formatting. For instance, a lot of merchants send us AVS data along with a transaction request. However, there are countries like France that won't utilize this data, yet you'll still pay a fee to Mastercard for submitting it.

So we'd suggest removing that to save you two cents per transaction. Of course, any of our recommended optimizations can be disabled or enabled, giving you the flexibility to customize your payment strategy.

ENABLING TOKENS

Use of **Network Tokens** is becoming industry best practice since Visa and Mastercard introduced theirs around a decade ago. While Network Tokens deliver business benefits – such as automatically updating expired card details – adjusting your tokenization strategy impacts your authorization rates, too.

Issuers want to see safe-looking transaction requests, and tokenized payloads are surely much more secure than those with the **PAN** exposed to the system. Tokenized payments can create better customer experiences in modern payment solutions like **one-click checkout**. Where card-on-file payments are tokenized, the buyer enjoys a speedier checkout compared with entering in their full FPAN details each time they revisit a merchant.

Our machine learning engine updates instantly to stay on top of issuer token adoption, adapting your payment tokenization to balance conversion and cost. That means Intelligent Acceptance will only apply Network Tokens as soon as the issuer in question supports them. The decision engine also takes into account whether the issuer has higher acceptance rates with tokenized payments rather than PAN credentials or there's a beneficial fee reduction.

DISCERNING ROUTING

As a large payment processor, we have a plethora of payment rail options to choose between. How do we choose which way to route your transactions? Our AI-driven decision-making engine **Intelligent Acceptance** continually learns the most effective payment rails for conversion. It's informed by more data points than any human team could ever calculate. Every failed payment is assessed and analyzed for potential improvements within milliseconds, boosting the chances of success for each one that follows. The same AI platform powers optimization and payment retries, which you can read about in the next chapter.

But we don't leave everything to the machines. Each of our merchants has optional routing rules to switch on and off. From our side, Checkout.com payments analysts will choose between different BINs and scheme rails, based on day-to-day experience with issuer acceptance and decline reasons.

For example, cards that are co-branded can be routed through either scheme on the card. Each of the schemes has different success rates and different costs, which our payment analysts are careful to monitor. Although the merchant would have no way of knowing what these are, we are happy to provide insight into how and why we're making decisions such as scheme routing. We know flexibility matters a lot to you, but so does trust, which is why we don't make traffic routing decisions without consulting with you first.

However, payment traffic flows are a collaborative process between ourselves and the merchant; you can take as much control as you choose. We always allow you the opportunity to change tack and maximize revenue according to your preferences – not ours. So there's a strong human element to our payment routing, and we never assume that machines know best. We collaborate with merchants to reach the best possible payment routing decisions, fine-tuned to meet your individual business goals.

03

REFINING RETRIES

Maxime Merabet
Principal Engineer, Retry Strategy

Failed payments don't always get the attention they deserve. It can be tempting to assume that all blocked transactions are obstructed for the right reasons – unauthorized card use, spoof payment details, suspicious account activity or one of the many types of cyber fraud.

We take fraud seriously (you can read more about that in the next section). And we also believe in maximizing merchant revenue. That means we make efforts to remedy wrongfully declined transactions using a combination of technological and manual refinements. A strong advantage we possess is the end-to-end management of the transaction process. As a payment gateway, 3DS requestor, and acquirer, we can retrieve more kinds of data to build a comprehensive picture of payment failures.

Moreover, our payments engineers are some of the best in the world. They appreciate the nuances in error codes in ISO8583 as well as EMVco, and what it takes to remedy each one. Every day, my team and I combine machine -assisted data processing with first-hand experience of payload configuration to successfully process transactions end-to-end. And we don't give up until we maximize legitimate payment success.

We do this all with cost efficiency in mind – saving merchants from excess fees.

While less sophisticated software will blindly retry payments over and over (racking up charges for each attempt), we calculate the precise moment your retries are most likely to succeed. Our Intelligent Acceptance engine also selects the path with the best chance of success, while ensuring the costs won't exceed the transaction value.

We'll outline some of the most successful strategies from short-term and long-term perspectives.

SHORT-TERM RETRIES

3DS Upgrades

Our Intelligent Acceptance engine calculates the likelihood of retry success following upgraded authentication by leveraging billions of data points from our transactional processing.

If a payment is declined for security failures, then we leverage different data fields such as merchant advice codes and our internal analytics gleaned from experimentation.

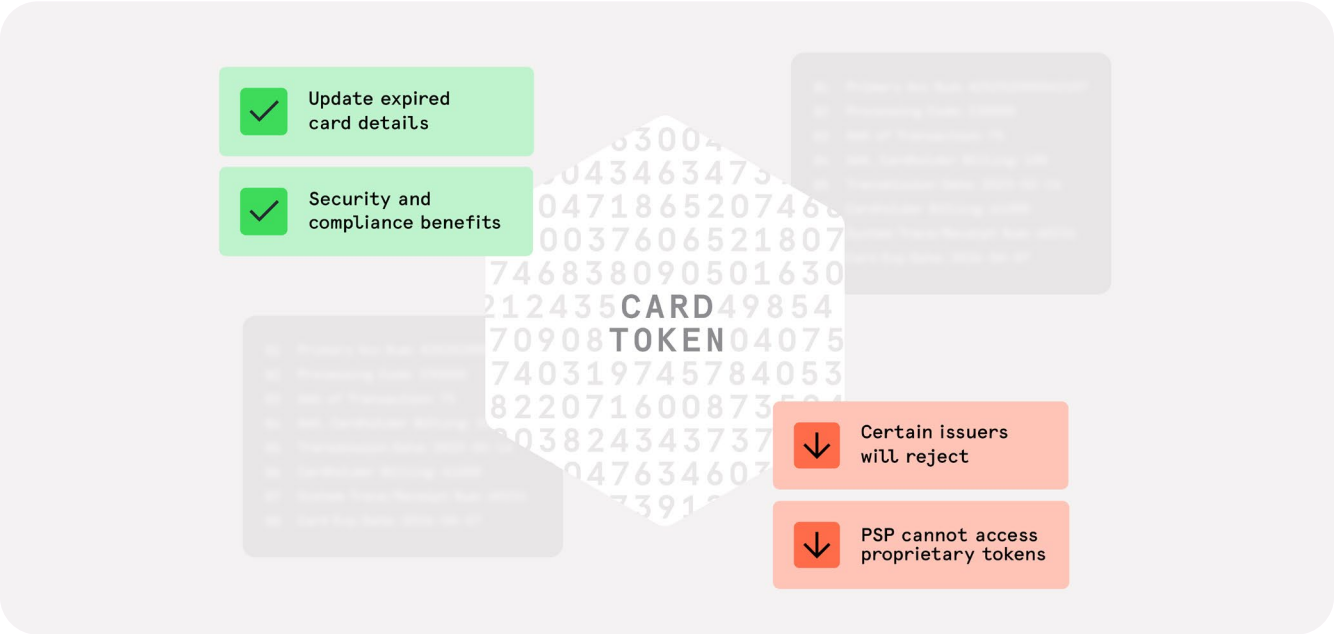
Over time, we have learned to judge where certain issuers favor transaction requests with given security levels, and can react accordingly. For instance, if an issuer declines a payment request over a certain security failure point, then we can instigate a 3DS request. This provides an opportunity to try and save the transaction, rather than deliver a decline response code and create a negative customer experience.

Payment tokens and fallback solutions

Tokenizing the cardholder's PAN delivers benefits for the entire payment flow. Tokens assist with data protection, offer a line of defense against criminal attacks, and update automatically when account details expire. Tokens can also deliver failed payments. Despite scheme mandate deadlines, some issuers (particularly the smaller ones) fail to update their tech in time for new tokenization mandates. Therefore retrying payments routing through certain issuers without the token will push them through.

Our ability to do this depends on the merchant's integration; if you're using tokens we can't access, then we're limited in fallback options.

Strategies around tokenization are particularly relevant to subscription-based payment models. Reason being the continuity of payment is vital to ongoing service provision, and there's nothing more frustrating for both customer and merchant than the interruption of ongoing payment collection.



When we can't tokenize certain cards, we can make use of our **Real-Time Account Updater**, which mitigates failed payments due to outdated account details. When a customer's card expires and they receive a new one, the scheme sends us a webhook which automatically updates the FPAN in our systems. This enables us to rescue payments that may otherwise have been lost due to incorrect card details. Combining both of these technologies means we can mitigate lifecycle-related problems to achieve greater acceptance rates.

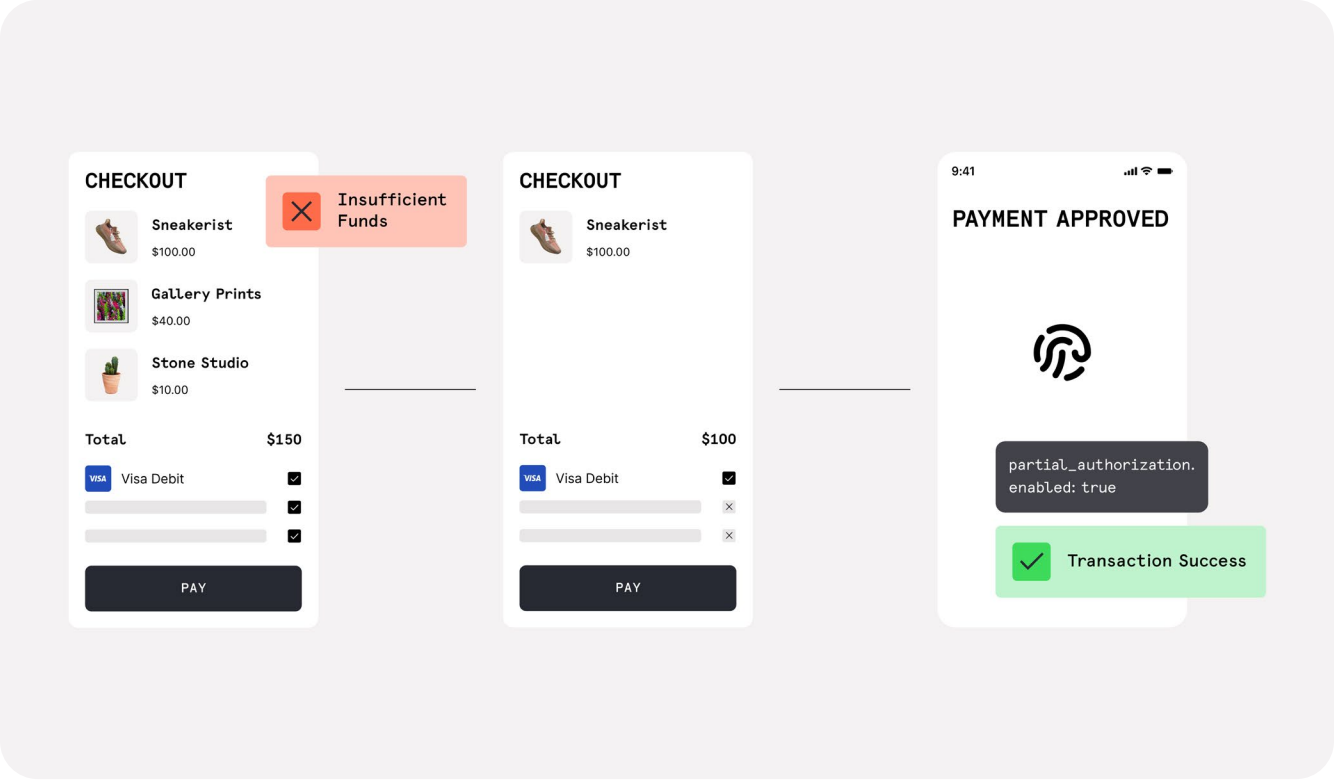
Partial authorizations that save failed payments

Legacy payment systems might attempt to take payment once, find insufficient funds in the payer's account, and deliver a "failed" response. The payment is declined and **45% of customers will not try the payment again**.

The payment is lost, and your customer is highly inclined to take their business elsewhere. he workaround might be to call or email the customer and ask them to try another payment method.

But that's not particularly efficient or cost-effective (nor is it guaranteed to work).

A smarter solution is to consider partial authorization. Aligning with card scheme and issuer mandates, a merchant can choose to capture an approved amount that is less than the total amount due.



The technique usually involves some negotiation with the end user, but this can be digitally managed. For example, a remittance service user attempts to transfer $100 to a South African account, but their balance is $78. Instead of declining the transaction, the issuer can support partial authorization of $78. That means the processor and payment gateway facilitate the opportunity for a new, lower-value transaction. With a simple pop-up message, the merchant can present the customer with an alternative remittance amount. This may be accepted, and the new transaction succeeds.

No decline message, no retry fee – just one more happy customer. In addition to the two strategies above, we rescue transactions and reduce merchant costs in a range of ways.
Let's look at some of those in more detail.

LONG-TERM RETRIES

Scheduled retries tailored to your strategy

Our dunning team carefully curates the intervals for retrying failed payments. Using such techniques, we recover around 30% of failed payments due to insufficient funds.

When we process a transaction that aims to recover funds, we specify a retry schedule to the gateway over a period of multiple days. This is particularly useful in cases such as insufficient funds or daily card limits, given that cardholder cash flow is unlikely to resolve itself within milliseconds of the first payment attempt.

From our wider network, we may be able to cross-reference the same payer with other transactions to predict their cash flow.

For instance, if a cardholder has just completed an expensive purchase for an ecommerce retailer (and the transaction came through us), then we can facilitate recovery of funds for a monthly subscription of a lower transaction amount.

We can also detect daily card limits from decline codes, and this informs us as to the next optimal payment retry window.

Nobody knows your business model better than you, of course. Which is why we encourage merchants to let us know how many payment attempts we should retry, and over which date range.

Close relationships with schemes and issuers

From our transaction throughput, we can pick up on patterns of declines that other payment processors would not be able to. And our daily communication with card schemes helps us to repair broken links in the chain, even at an issuer compliance level.

For instance, we noticed a European issuer was declining tokenized transactions with an expired card decline. However, the token was still active, which pointed to poor lifecycle management in the issuer's systems. We realized we needed to implement retries with the full PAN, in order to get those payments through. To remedy the issue long-term, our engineer flagged this to the scheme, who then deployed a task force to strengthen acceptance rates.

We achieved around a 90% retry success rate as a result of that particular feedback loop.

And that's just one example of many instances where our relationships with schemes improve transaction flow for the wider payment ecosystem.

Such close ties mean we're the first to know when schemes release new mandates and regulators require new protocols. At the nexus of this interchange, we ensure no payment oes astray.

Such expertise is particularly valuable in the fintech space because we are keenly aware of mandates around signing, transaction tagging, and other technological specifications. We're the first to know when payment industry requirements are changing, and our merchants are the first to benefit from efficiencies in the process.

04

FRAUD & DISPUTE FEEDBACK LOOP


Daniel Linder
Senior Director, Payment Performance


Alexia Le Tarnec
Product Manager, Disputes

Fraud does not stand apart from your acceptance rate; there is a direct relationship between the two. On the one hand, your fraud monitoring informs PSP decision-making on how to route payments and when to request authentication. On the other hand, schemes and issuers interpret your payment traffic partly based on your reputation for fraud.

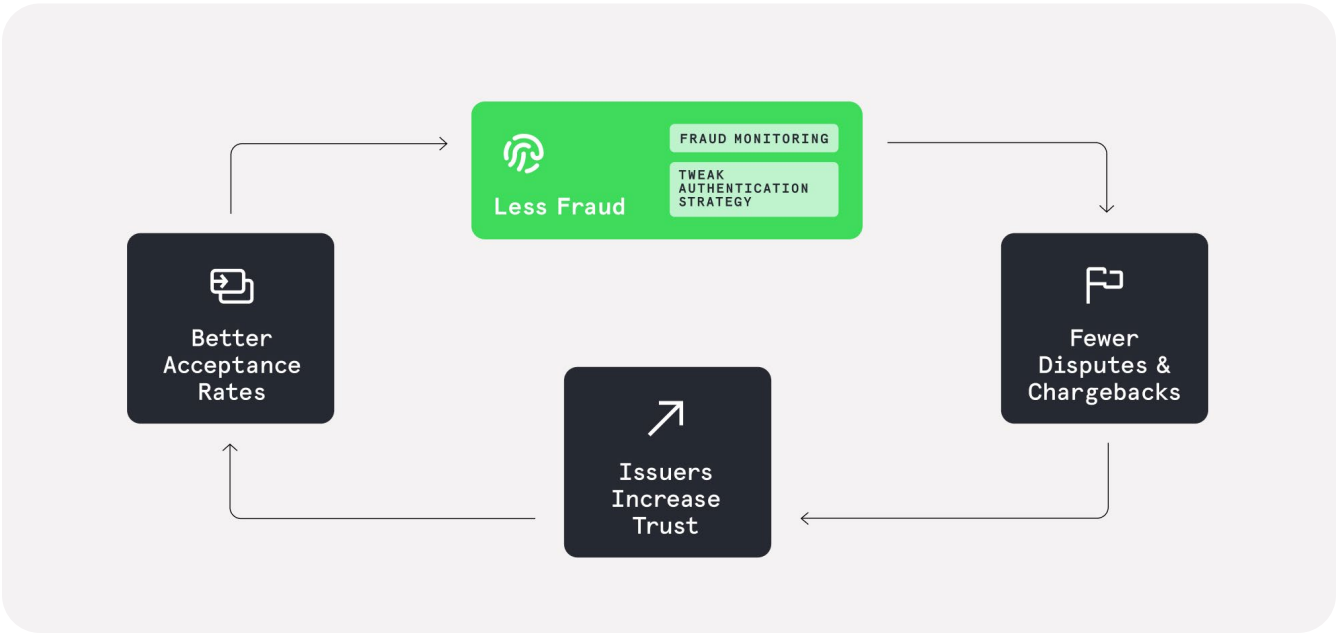
There are different ways to calculate your payments acceptance rate, and not every merchant is factoring in their disputed payments. But even if you don't, the issuers will.

When it comes to improving your business revenue, your appetite for fraud risk plus your strategy on payment disputes are critical.

Yet a concerning majority (64%) of merchants do not receive any fraud or chargeback analytics from their PSP. It's very hard to fix what you don't know is broken.

To begin addressing this, consider your historical fraud and dispute rates. Know that issuers, schemes and processors assess your trustworthiness based partly upon whether or not you have been, or are currently on, a scheme monitoring program.

Indeed, there is no successful payment strategy that omits fraud prevention. So let's look at how you can improve payment success rates by carefully working to reduce fraud.



CUSTOMIZING YOUR FRAUD RISK BLOCKING

You won't find fraud unless you look for it. And turning a blind eye to **fraudulent payment activity is a revenue risk** your business can't afford.

Although you can choose to have a standalone fraud monitoring tool, it's going to take some careful engineering to connect your financial systems with it. On the other hand, a combined solution such as Checkout.com's integrated Fraud Detection Pro eliminates the risk of an incomplete picture based on disconnected data.

A fraud engine directly connected to your payments systems can implement protective measures instantaneously.

And an industry-leading solution is flexible enough to incorporate **custom rule sets** based on customer segmentation.

As you scale your business, that means you can configure more lenient authentication rules for repeat customers while maintaining tighter controls on new payers.

You may also wish to consider additional security features on your own website, such as preventing too many purchases within a short timeframe or initiating checks on high ticket purchases from new customers. It can be worth having a block list on IP address or device ID for certain repeat offenders.

CUTTING DOWN CARD FRAUD

There are many ways to reduce bad actors attempting to use stolen payment details. Authentication is always the strongest line of defense; you can read more about 3DS strategies in Chapter 1. Sometimes the issuer will still raise a fraudulent payment dispute even if the payment was authenticated with 3DS.

In such cases, we represent the dispute on your behalf. To keep your systems secure, utilize a combination of automation, machine learning, and custom rule-setting with an adaptive fraud monitoring solution such as **Fraud Detection Pro**.

While all kinds of fraud are reduced with 3DS, certain vendors rely on a low-challenge payment experience for a positive customer experience. We recognize the importance of tailoring your fraud rules to your business goals, which is why we're offering a few different perspectives, here. You should consider a blend of business operations, customer service, technology, and process-related techniques to combat the rate of your payments marked as fraudulent.

MORE PIECES OF THE PUZZLE

When it comes to fraud assessment, there's no such thing as too much information. So you can help us to help you by bulking out your payloads with customer details and device information.

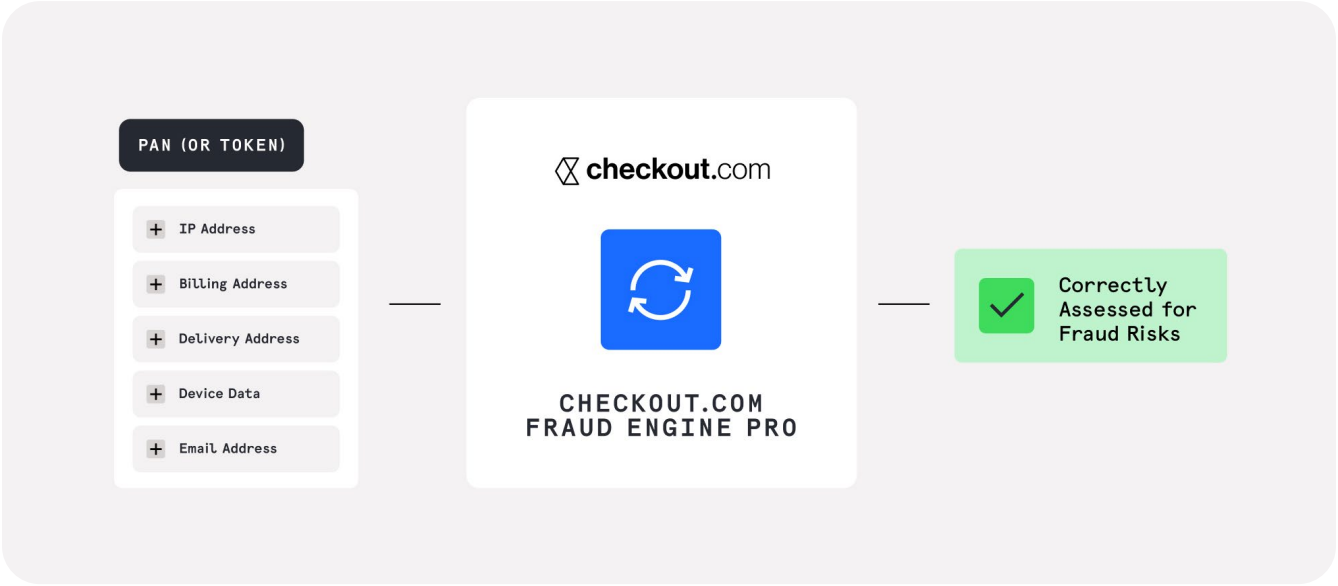
Let's visualize this with two examples. The first payload contains the FPAN (funding primary account number), transaction amount, and cardholder name. We could assess velocity features, and weigh up how well the transaction amount matches the merchant's AOV (average order volume). We'll check whether the same FPAN is connected to previous payments – and if any of those were disputed. Using these measures, we can assess fraud risk pretty well. But with more data? We can go further.

We know, for instance, that a cardholder making a transaction request in France cannot suddenly appear in Japan one hour later for another payment.

That's why fraud detection is even stronger if you include location, device data, and IP address in your payloads.

With a few more pieces of the puzzle, fraudulent payments become easier to identify. One of our ecommerce retailers saw an 8% reduction in fraud after adding in the shipping address to payloads.

With additional data, you give your fraud tools, PSPs, and issuers the best chances of accurately detecting fraudulent payment requests. This doesn't always have to mean a strong authentication challenge every time your customer wants to make a payment; one of our gaming merchants saw an AR uplift of nearly 2% by sharing customer details securely with us.



Here's a summary of useful payment-adjacent data that you can send to your payment processor to assist with fraud prevention:

- **Customer name:** this is important for us to verify account details with the issuer. We also check to see if the name is likely to be spam (such as a string of random letters) or if the name is associated with any fraudulent transactions in the past.
- **IP address:** it's useful to check whether the IP address has previously been flagged for fraud, and if it matches the general global region of the billing address.
- **Billing address:** we can submit an **AVS** request to check whether the customer's billing address matches the data their bank holds.
- **Delivery address:** a delivery address may not make sense for the MCC. Say the merchant sells designer fashion goods. A residential delivery address that matches the billing address registers low on the suspicion scale. On the other hand, delivery to a park or a bus station is rather suspect.
- **Email:** we can check whether fraud has been associated with this email address previously, and whether or not there is anything suspicious about the email address itself.

Truthfully, it's tough to win payment disputes categorized as fraudulent. You have a better chance of winning any other type of dispute claim. That's why it's critical to target fraud at the source – before it hurts your customer, and (ideally) before it reaches the issuer.

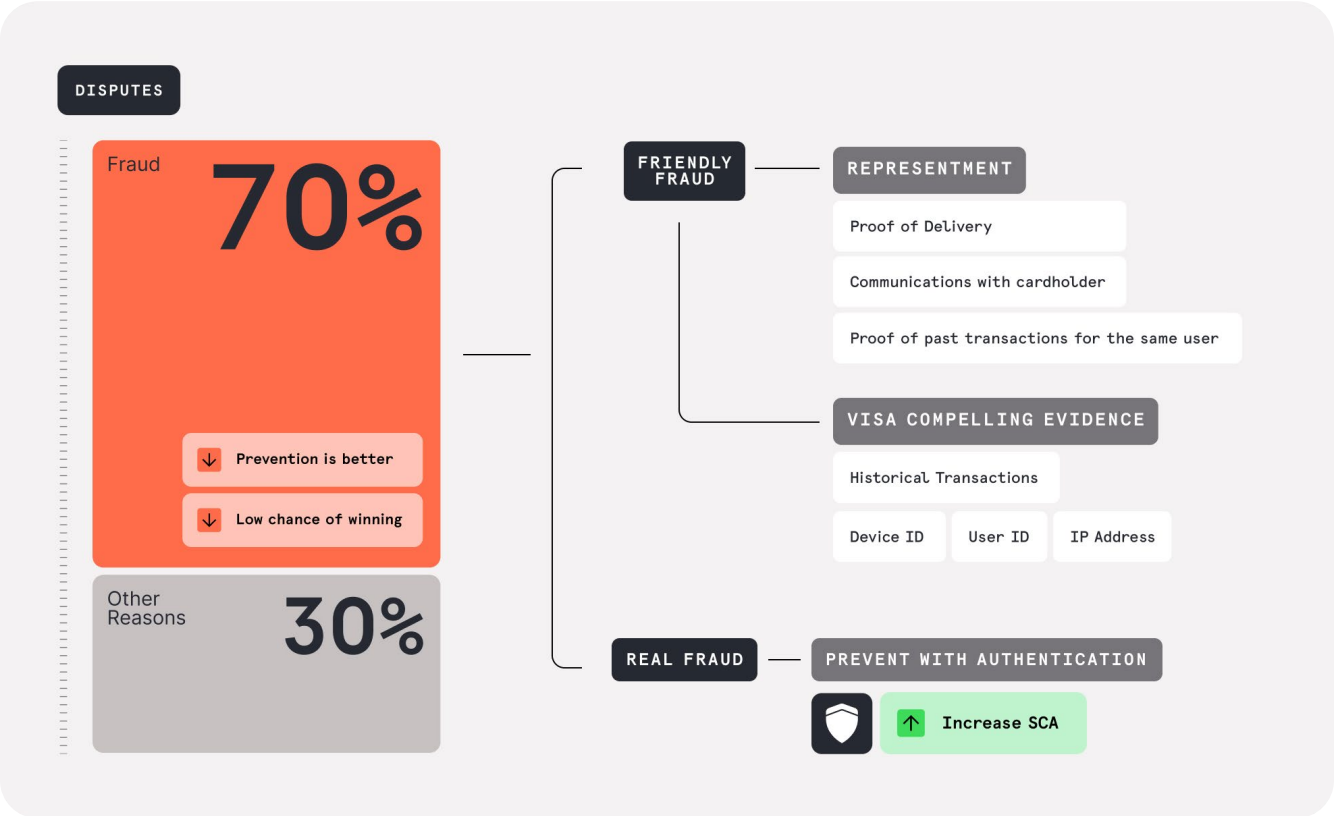
FIGHTING FRIENDLY FRAUD

Around 70% of the disputes we receive for merchants arise from fraud. Of these, we estimate at least 50% could be friendly fraud, which can benefit from a different approach compared with tackling fraud committed by a third party.

Friendly fraud may arise from confusion rather than ill intent; it can include genuine payments that the customer forgets about, and then disputes out of concern they've been a victim of fraud. Customer service plays a role here: sometimes a quick email or phone call can be enough to remind the customer that you can process a refund without a formal payment dispute.

There are some technical additions you can implement, too. For instance, adding a billing descriptor to card transactions can help to reduce disputes caused by unrecognized transactions.

If you customize the text displayed on the customer's card statement to relate to the purchase (such as naming the software package or subscription purchased), you can help avoid confusion over legitimate charges.



You can also automate beneficial data collection with **Risk SDK**, and include device fingerprint, device IP, browser type, and more using the integration. The data is already generated from the simple fact your customer is using a particular device to access your business's goods or services over the internet.

If it provides a secure, easy way to improve payment success, then it's certainly worth considering for your business.

If the above tactics fail, and the customer presses ahead with their dispute claim, then you will need to present evidence at the **representment** stage. This can include proof of delivery, previous similar purchases from the cardholder, and any other relevant communications with the customer.

If your customer paid with Visa, then you should look into our explainer guide on the **Visa Compelling Evidence 3.0 process** for disputing card-not-present transactions.

CONCLUSION AND KEY TAKEAWAYS

When it comes to improving acceptance rates, there's a strong theme of including sufficient data in your payloads. Submitting a more well-rounded transaction request to the Checkout.com API is helpful on a number of levels: more data means better fraud filtering, reduced chargeback risk, and smarter payment routing decisions. You can help us to help you by considering whether there are more types of data you could include in payment requests to our API.

Another key takeaway is the importance of well-informed traffic direction.

We firmly believe there is no strong decision-making without data. Which is why you need a PSP that's transparent with how, where, when, and why they're choosing certain payment traffic routes on your behalf.

Our advice is to probe your payment processing partner on exactly which optimizations are taking place on your traffic, and how much say you have over nuances in that strategy.