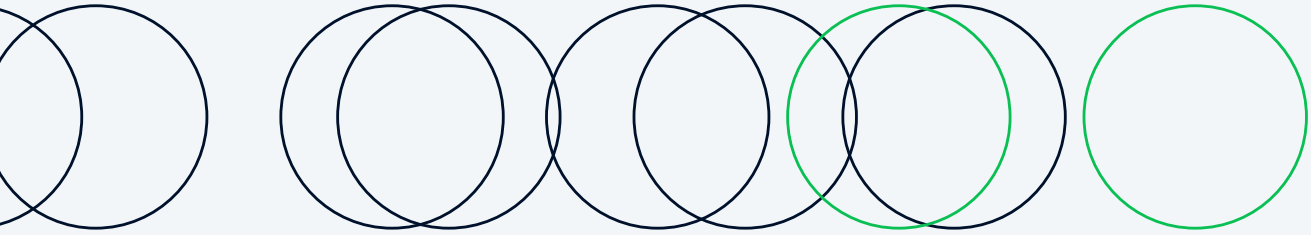
Guide

Accept, Process, Protect, Recover

Marginal Gains with payments



adyen

Whether it's attempting to win the world hotdog eating competition or Olympic gold in cycling, achieving greater productivity or even overall health: small, incremental, continuous improvements can add up to make big changes.

Dave Brailsford, former performance director for British Cycling, is perhaps the greatest modern proponent of marginal gains. He believed that by making 1% improvement in a whole host of areas, the cumulative gains would end up being hugely significant. This is also the case for improving your payments.

Originally featured as a series of blog posts, this guide covers four of the most important factors to consider when approaching payments: Accepting, processing, protecting, and recovering. We'll look at what you need to know, what Adyen offers to help, and some of the benefits we've provided to our partners.

Accept Process Protect Recover

First, let's explore what you can do to keep authorization rates high and accept the highest possible percentage of payments.

Making gains by optimizing payments

Optimizing payments can mean a variety of things. It could mean offering the right payment methods in relevant markets, intelligently authenticating customers, all the way through to implementing regulatory requirements. Expertise and technology are equally important.

Optimize with payment methods

Geography, demographic, context. These are three of the most important things to be aware of when deciding on the best mix of payment methods to offer your customers. Here's why:

Things to think about	Why?	The gain?
Geography	Payment method usage varies from country to continent, and their popularity can be dependent on many factors. In Kenya, it could be a lack of access to banking facilities, while in the Netherlands, it could be due to an aversion to credit cards.	Take M-Pesa's popularity in East Africa. In a region where 91 million (or 17%) people don't have a bank account but 75% have mobile phones, M-Pesa succeeds in being a mobile network operator that allows users to make payments, transfer money, and microfinance purchases.
Demographic	Gen Z'ers and boomers differ in more than age and outlook.	If the first impression millennial shoppers make is via a social media platform, then retailers should utilize social media for payment.
Context	Assess how your product or service might impact the payment method your customers choose. For instance, the way we buy a car differs from the way we buy a scone.	We encourage merchants to experiment with payment methods based on their needs. Through our merchant network, we have a range of performance insights. So regardless of industry, business types, and countries to help you get an optimal mix.

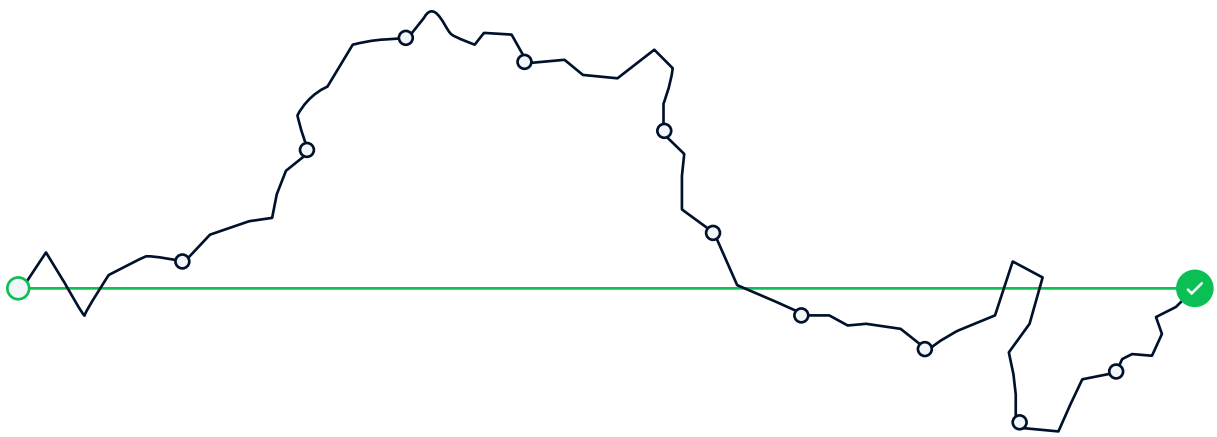
Learn more: payment method guides ›

Accept Process Protect Recover

Optimizing the authentication experience in times of PSD2

Once the shopper has hit “pay,” authentication may come into play. Conversion is now your number one concern, followed by meeting regulatory requirements like The Revised Payment Services Directive (PSD2). PSD2 is a European regulation introduced to make payments more secure.

We developed our 3D Secure 2 (3DS2) solution to improve authentication flows and save businesses time figuring out the different regulatory landscapes in each region. It also makes the authentication process less tedious for customers.



Accept

Process Protect Recover

3DS2 makes it easier to accept payments. The combination of certified SDKs in the checkout flow, paired with data-sharing APIs, means that merchants and banks can share data in the background with limited interruption to the customer's checkout experience. The option to build a native 3DS2 experience limits the need for shopper redirects to a non-native authentication page.

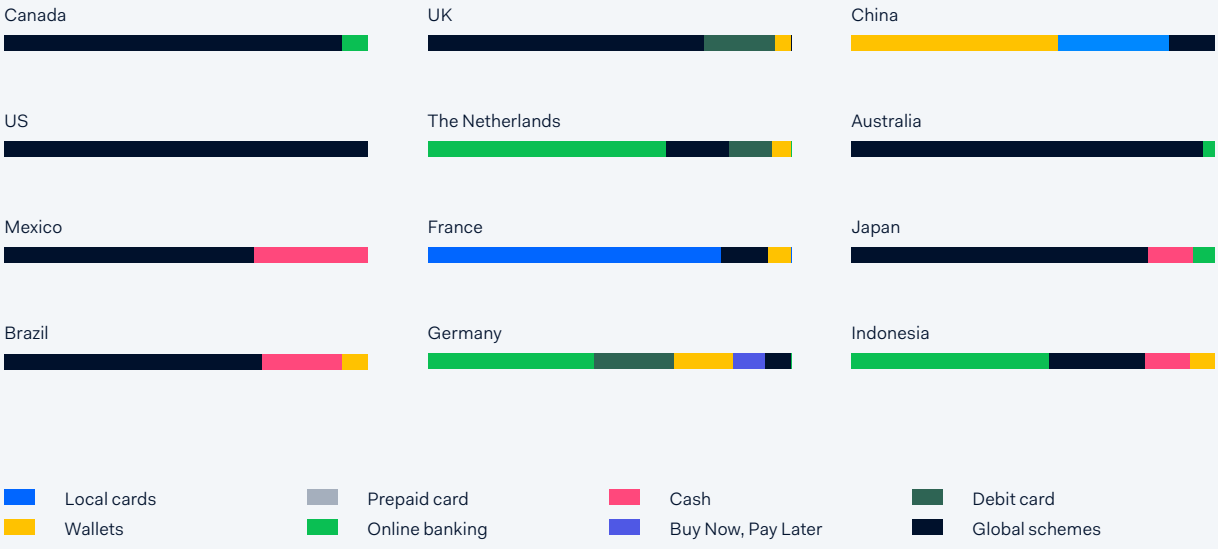
In short, it optimizes the checkout and often increases authorization rates.

For payments involving European shoppers, PSD2's Strong Customer Authentication (SCA) is required. These are 'something you know', 'something you own', or 'something you are'. This combination makes authorization easier because, well, you can't forget your thumbprint, can you?

There are also a couple of exemptions that can make things even more straightforward.

1. Low risk, low value, and subscription-based payments are exempt from SCA
2. Shoppers also now have the option to select a list of 'trusted beneficiaries' that can be saved by their bank, so that they forgo 3D Secure.

How the world likes to pay

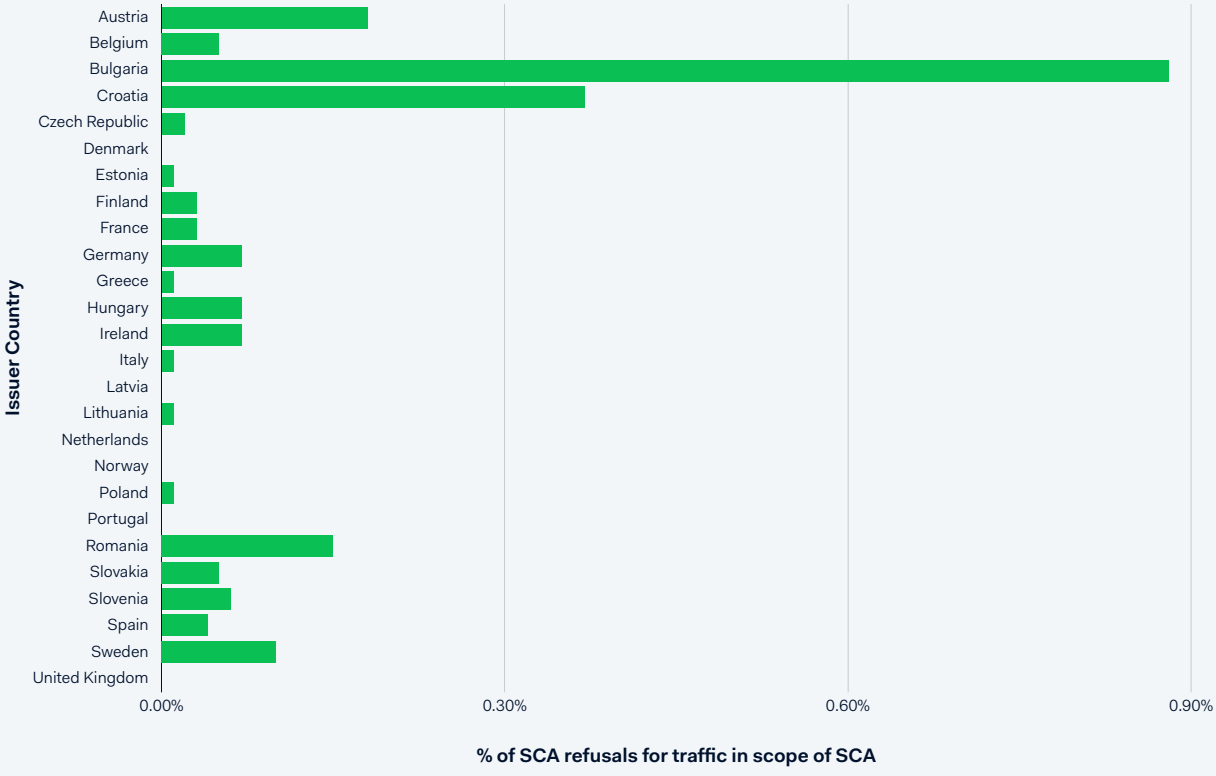


Accept Process Protect Recover

The route to higher authorization rates

We built our Authentication Engine to simplify the route to higher authorization rates. We do this by monitoring and identifying patterns and behaviors, then acting upon them in real-time.

The chart below illustrates the percentage of declined payments due to SCA requirements ahead of PSD2 enforcement deadlines. Using our Authentication Engine, these payments will be automatically retried with SCA so that the shopper can complete their purchase.



Accept Process Protect Recover

There are key aspects to look for when understanding how authentication application can be optimized:

Funneling the authentication flow

There are two checkpoints to a payment: authentication and authorization. It's at the cross-section of these two checkpoints that 3DS comes into play.

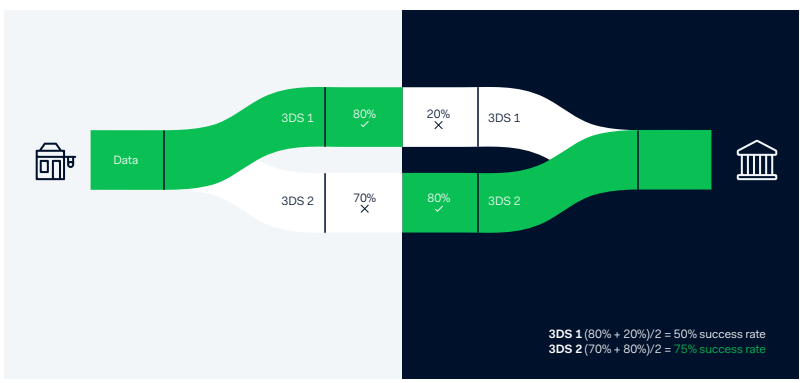
Checkpoint 1:

Authentication and the merchant. The provider of your 3DS2 solution knows what works best for your business and customers. This can be based on locale, payment method, device, and more.

Checkpoint 2:

Authorization and the acquirer. When it comes to card issuers, the acquirer knows what version of 3DS works best for the highest authorization rates. The merchant and acquirer are often separate entities, which can cause a disconnect and a higher likelihood of declined payments.

Every payment is unique, so a full view of the transaction can be really important when striving for the highest authorization rates. This is the basis of our end-to-end solution.



Adyen tips:

Apply exemptions within the payment process. These reduce the risk of declined payments by an issuer and the merchant having to process the payment twice. Processing a payment twice can be costly; it means two transactions, twice the costs, and the potential to inconvenience your customer.

Make sure you're up to date from a regulatory standpoint. Look for options that use machine learning to assess large datasets and optimize in real-time. This means you don't lose out just because an issuer has made a change at their end or if a new exemption comes into play.

Accept **Process** Protect Recover

Today, there are many different ways for businesses to send a payment to an issuing bank, and each of these issuing banks has its own tech platforms and procedures. It's like riding a mountain stage of the Tour de France: unforgiving for the uninitiated, awash with complexity, and even harder to manoeuvre when you're hindered by out-of-date technology. The road to success has been a bumpy, uphill battle for many merchants. But in recent years, we've seen massive strides in how payments are processed, so it's time to change gears.

Let's take a look at some effective ways to boost your processing and the products Adyen offers to help.

Étape 1: Get the best route with local acquiring

The best solution for processing payments is often found by working alongside one partner with local acquiring licenses for all the markets in which you operate.

How local acquiring can get you ahead of the pack

Payments processed using local acquiring can cost less and are more likely to be authorized. By using Adyen acquiring, you can track payment methods, performance, spot trends, and get to know your loyal customers.

Learn more: Cross-border payments ›

Using Adyen for acquiring also means access to RevenueAccelerate and its features, including Network Token Optimization.

Delivery Hero

"Having leveraged Adyen's local acquiring solution in other markets, we are excited to enjoy the same benefits in Malaysia including a more than 3% increase in authorization rates."

Franziska Bubl — Senior Global Payments Manager, Delivery Hero

Accept **Process** Protect Recover

Étape 2: Power your processing with performance-enhancing Network Tokens

Saving payment card details is revolutionizing how we pay online.

Network Tokens are a secure card token from EMVCo, replacing the card number (PAN) for payments. They were originally developed to maintain security while preventing payment disruption when it came to card expiry. They're maintained by card networks, available in upwards of 150 countries, and automatically updated when a shopper's card details change. This, and the use of Adyen's Account Updater, offer a simple way for businesses to access up-to-date card information in real-time.

Benefits of Network Tokens

Available in over 150 countries	✓
Hides card number (PAN) for improved security	✓
Automatically update when shopper card details expire	✓
Maintained by card networks	✓
Out of PCI scope	✓
Higher authorization rates	✓

New technology to solve old problems

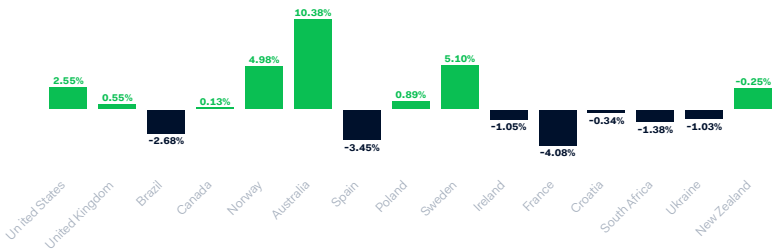
Network Tokens are a recent innovation, built with the goal of eventually replacing account numbers. In the long term, businesses may be able to skip the costly and time-intensive PCI certification, freeing up time to focus on what they're good at.

Learn more: What PCI stands for and how to become PCI compliant ›

Despite the obvious benefits, issuing banks can still be apprehensive when implementing Network Tokens. Issuers need to build the capability to approve Network Tokenized transactions, meaning that while some markets see a high number of issuers building with tokens in mind, some aren't ready. Additionally, not all issuers authorize Network Tokens on par with PAN authorizations, so there's potential for a drop in authorization rates if an intelligent approach to routing isn't applied. Fear not though, this is where Network Token optimization comes in.

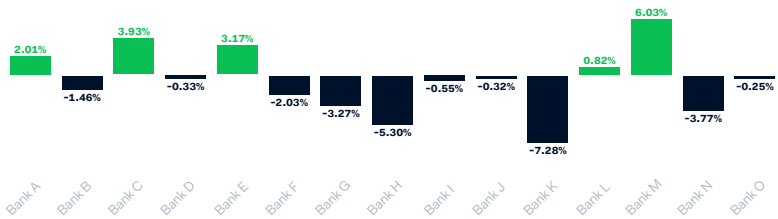
Why Network Token Optimization is needed

In the chart below, we show Network Token adoption across different regions and the uplift (or decrease) in authorization rates they bring. Sweden is a case in point. With the country's propensity to prefer cashless payment methods, authorization rates increase by 5% if you offer Network Tokens with intelligent routing. Look at the UK however, and you see a smaller increase.



Accept **Process** Protect Recover

This isn't the full story though. While illustrating a small 0.55% increase across payments in the UK, the chart below also shows that the issuing banks utilizing Network Tokens are experiencing great uplift.



With Network Token Optimization, we can decide when to use a Network Token versus a PAN, based on our machine learning capabilities and platform data. We only send Network Tokens if it's the issuer's preference, and even if the shopper's card is declined, we can immediately retry with the PAN.

Étape 3: Smart Payment Messaging for the fastest finish

Consumers have borne the brunt of all the crossed wires and confusion that surround processing payments. Time and time again they've seen their checkouts interrupted, subscriptions terminated, and payments incorrectly blocked. What this calls for is a continuously learning engine that modifies payment messages to each issuer's liking.

Smart Payment Messaging is a feature of our payment experience tool, RevenueAccelerate. We adapt the format of payment messages to best suit an issuing bank's preferences.

We automatically reformat the data sent with each payment request according to the issuing bank's specific preferences and past behavior. This could be in the form of a card expiry date or a shopper's address. Smart Payment Messaging is at its most effective in complex payment environments or where outdated issuing banks are prevalent.

The best fit for new regulations

When banks don't update to incorporate the latest card network regulations, things can get complex. We saw this happen with the introduction of new card-on-file indicators by Visa and Mastercard in 2018. Some banks neglected these updates, leading to a significant number of declined payments. Smart Payment Messaging can mitigate this by recognizing changes and adapting the payment message to the old format for such banks, leading to approved payments and happy shoppers.

Other banks have non-standard behavior when it comes to receiving authentication data. In 2020, a new regulatory requirement meant that data needed to be sent in a different way to banks; in a slightly different place in the payment message; yes it can get that complicated. Some banks haven't adapted to this yet, and again we've discovered smart payment messaging racing to the rescue.

How payment messaging can sustain your growth journey

Issuers decide to approve or decline a payment based on the data contained in payment messages. Tweaking these messages can be the difference between a happy customer, and one that never returns.

Nevertheless, as issuers' preferences change, so does our Smart Payment Messaging. This means that authorization rates stay up even if an issuer turns its system upside down.

Out of the mountains and onto the track

The hard part is over; you've learned what's on offer when it comes to processing payments. So whether it's with messaging, acquiring, or Network Tokens, make sure you're using what's available to make those marginal gains.

Accept Process **Protect** Recover

For track cyclists, their safety is in their speed. Riding slow and without intensity could mean a last-place finish, or worse still, the risk of a crash or dismount. As such, everything related to the track is fast but safe; aerodynamic helmets, clip-on pedals, right the way through to the curve of the velodrome.

Until recently, many ecommerce businesses prioritized security ahead of customer experience, with many payment providers applying a less-than-perfect, slowed-down approach to combat fraud, blocking payments at the slightest sniff of inconsistency.

In this chapter, we'll explore ways to optimize security, use risk management tools, and how to implement advanced algorithms and shopper recognition to get the best authorization rates.

The risk management tech that keeps the wheels turning

Some providers recommend a hardline on safety, ultimately turning away genuine shoppers while promoting a '0% chargeback guarantee.' Other providers position new advancements in machine learning, AI, biometrics, and even PSD2 SCA regulation as magical fixes.

We believe that there's no such thing as a silver bullet and that the best way to protect shoppers is by combining different techniques to make the best risk decisions.

Recalibrate in shifting environments

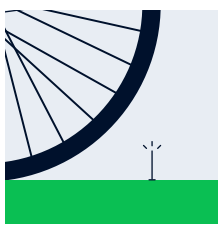
Riders tweak their bikes as they move from the sprint to the mountain stage. The same goes for the changing fraud terrain that we see daily. Ecommerce fraud used to be all about hacking the payment gateway and stealing card details, but this has evolved in recent years. It's now a battle against both automated and human-driven attacks.

The emergence of click-farms and bots is one such story. Ten years ago, very few people knew what these were, today they're commonplace, influencing everything from reality TV, to elections, to payment fraud, coordinating a high velocity of automated attacks to yield results. They're real-world, physical sweatshops where fraudsters employ staff to conduct focused attacks by presenting themselves as real shoppers. Workers combine a range of data points (a date of birth, a password leaked in a data breach, or a postal address) to sign-in, then access any available payment or identity details.

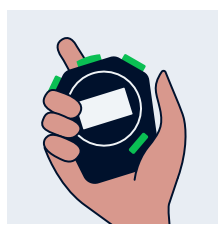
If you can't calibrate fraud across both automated and human-driven attacks, you'll fall behind the pack and lose trust with shoppers. That's enough of the scary stories though; it's time to see what businesses can do to fight back and get ahead of the fraudsters.

Combining the components to build a winning machine

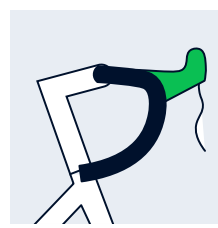
There are five components that you should look for when building your risk management system. Some are obvious (fraud detection tech), and others might be new to you (testing and experimentation). Let's take a closer look at these components and their features.



1. Fraud detection technology



2. Supervised machine learning



3. Customizable settings for your business

4. Testing and experimentation

5. Cost efficient risk operations

1. Fraud detection technology

Your first step in preventing fraud is the ability to detect it. Most fraud detection technology uses advanced data science, utilizing machine learning models to detect behavioral abnormalities across a range of data sets. The technology can be configured for specific high-risk segments, gambling for example, or geographic regions with higher fraud rates.

We recommend finding a provider that utilizes multiple machine learning models and theories used to detect fraud. This way, you cover all possibilities and avoid unintentional biases regarding locale, payment method, or transaction value.

2. Using risk knowledge and data to fight fraud

Using the combination of your own risk knowledge and that of the machine is known as 'supervised machine learning'. Supervised machine learning uses labeled data, payment authorization details, and thousands of other data points when making decisions. The machine is 'rewarded' based on its success (each correctly blocked fraudulent transaction), so it doesn't rely on predetermined ideas or notions like humans would.

The idea is that by starting with a base of information, the machine learns and adapts to a multitude of fraud situations.

Providers with a long history of risk management, international coverage, as well as access to comprehensive transaction and shopper data often mean the machine holds better judgment and results. Ensure your provider is continuously training the machine to go up the gears as the fraud terrain changes.

Remember that with supervised machine learning, the machine is only as good as the base data. If there are anomalies or unique reasons to block a payment, the human approach is still important to consider.

3. Customizable settings to support the needs of your business

Companies and industries can learn from one another, especially when detecting certain types of fraud.

Take streaming services with a freemium pricing model; these businesses may experience many card testing attacks. Similarly, you might be a sports retailer launching a hot sneaker drop when a bot attacks to buy up stock before real shoppers can. This is where industry risk templates come in handy, giving you a somewhat tailored guide based on your industry. It's not a blanket approach either, with the right risk management platform you can build on the template by adding customized risk rules.

Risk rules make it easy to apply customizable settings, and allow you to trigger an alert or to complete an automatic action like sending the transaction to review queues or decline a payment. Adding and adapting these help you to respond to changing internal risk appetites, market seasonality and set hard no-go rules for your business. You can also manually override machine learning rules with your own custom rules when applicable.

At Adyen, we also provide suggested custom rules based on learnings from our merchant network. We can apply said rules at a campaign level. E.g., for limited edition items, like the aforementioned hot sneaker drop, add a block rule so shoppers can only purchase one item.

Accept Process **Protect** Recover

4. The ability to test and experiment from the outset

Conducting regular A/B testing is one way to continuously strengthen your risk settings, ensuring that you protect your customers as fraud evolves.

When experimenting, setting a clear hypothesis is vital, but it's also important to set significant sample sizes. You can achieve this by running tests longer, using smaller segments so you can see lagging indicators, or choosing groups you'd like to test with, e.g., specific geographies on a larger scale over less time.

Look for a provider that lets you set A/B testing, define the target segment and get recommendations on how large a sample size needs to be so the experiment is worthwhile. Factor in things like seasonality (i.e., don't run a general experiment during Black Friday) and understand how to extrapolate results to make meaningful changes based on your tests.

5. Cost-efficient risk operations

We know fraud isn't always black and white and that if it isn't click-farms or bots, it's an over-enthusiastic shopper with a slow internet connection. It's essential to have the ability to optimize your risk management flows and to make sound review decisions promptly. Customizing and segmenting your support queues allow you to control the flow of cases by routing traffic to the correct support agents.

The ability to review payments with the relevant information is key, so use a provider that integrates third-party databases such as postcode checkers, social media snippets, and other verification databases.

Related: Beating payments fraud

Protected right away

It isn't always possible to detect fraud, but you can fight back, and it's all about the small incremental improvements, whether with machine learning, experimentation, or regulatory safeguards. Think of the cyclist's literal and physical risk management; their aerodynamic bike, healthiest diet, and the latest in helmet design protect them on their way. They might crash every once in a while, but they'll finish the race and keep getting better.

Accept Process Protect **Recover**

In this chapter, we'll look at recovery. We're not talking about ice packs and rest days though; we're talking about reacting to setbacks; how quickly you can recover from a puncture, a fall, a collision. Or in payments; recovering from failed transactions.

Why payments get declined

We don't want to state the obvious too much here. But it's important to highlight that there's no blame game when it comes to declines.

Insufficient funds

We've all been there. A few subscriptions going out of the bank account just before pay day. In fact, 72% of declined transactions are due to insufficient funds or 'do not honor' codes.

Technical reasons

What shoppers don't often see are the errors between the card schemes and issuers. These lead to 'technical error' messages. Similarly on the backend, the payment form can time out, and cause the shopper to drop out of the payment flow.

Wrongly formatted messaging

Each issuing bank has different risk preferences and technologies, and these preferences extend to messaging. For example data such as CVC and/or expiry data formatting.

Accept Process Protect **Recover**

How to recover declined payments

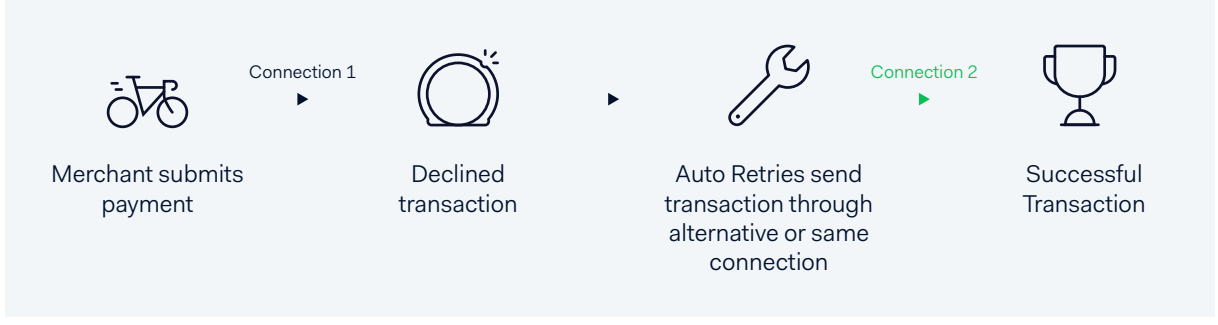
As we covered above, there are multiple reasons why you might need to recover a payment. But it needn't be a manual process. We have two specific solutions: Auto retries and Auto Rescue. Auto retries are attempted immediately after the first decline whereas for auto rescue this is a longer timeframe (another day/time).

Auto retries

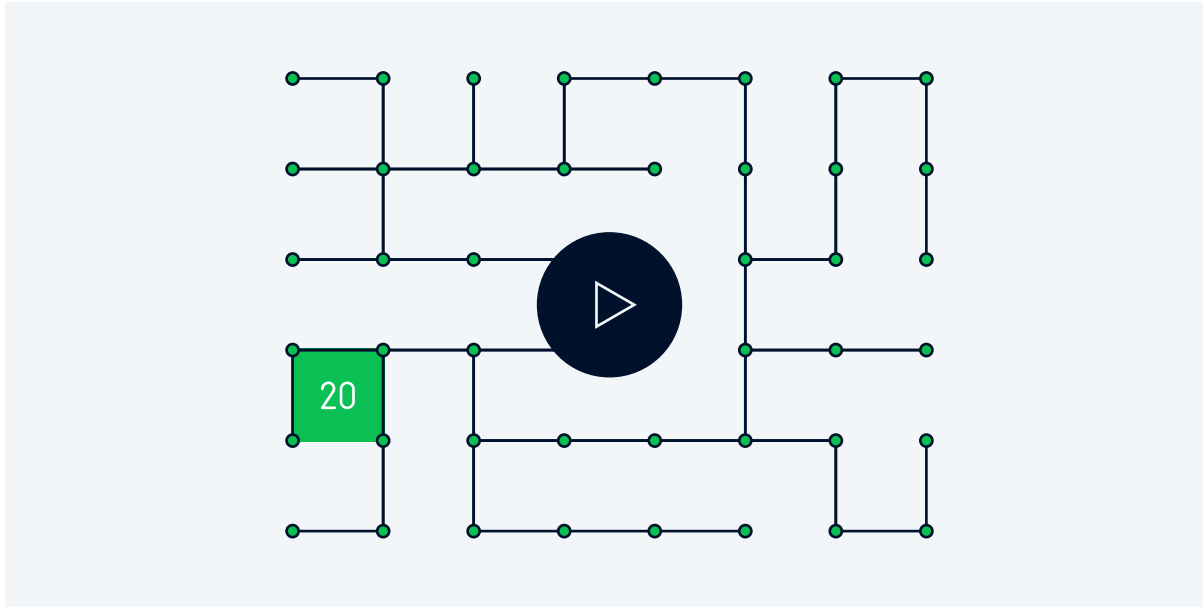
Auto retries are a feature of RevenueAccelerate, enabling us to retry previously declined payments due to technical errors. The retries are attempted immediately after the first decline, meaning shoppers don't need to re-enter their details. It's especially helpful for retail and food delivery businesses.

We do this through the same or a secondary connection, using our platform data to retry only when there is a high chance of success and preventing your business from incurring extra card network fees.

We all know that risk management is a continuous process. Stop pedalling, and you'll be caught. This is why we're always improving features like Auto retries.



Accept Protect Process **Recover**



Not-so-marginal gain: The introduction of machine learning to auto retries

One of the questions we're most commonly asked is how to keep costs down, especially when it comes to retries. With machine learning we can determine how best to format them, and when not to retry at all.

Since we started using machine learning to support auto retries in July 2021, we've seen a 300% increase of recovered payments.

Accept Protect Process **Recover**

Auto Rescue

Auto Rescue recovers declined payments through automated, intelligent retries. This is particularly useful for shopper-not-present transactions such as subscription renewals. It uses smart logic, using our wide range of payments data, to decide which declined payments can succeed when retried later, and performs these retries at optimal times on behalf of your business. It's easy to integrate too; you can simply update the payment API to flag a transaction for Auto Rescue and we'll handle the rest, providing notifications on the outcome of each Rescue attempt. Auto-rescue was originally available for card payments only, but we've recently expanded its scope to incorporate SEPA payments as well.

Unlike Auto retries, Auto Rescue re-attempts the payment at a later time or date, making the feature ideal for subscription businesses.

Leveraging the payments community to make subscriptions unstoppable ›

Not-so-marginal gain: Recover payments declined due to insufficient funds

We use our PSP-wide data to schedule retries factoring in parameters such as Bank Identification Number (BIN), country, and decline reason. This enables us to pinpoint what day of the month, day of the week, and time of the day to schedule a retry to match when shoppers are most likely to have money in their bank account.

You've made it to the finish line

The ability to accept, process, protect, and recover payments are four things every business should have at the top of their mind. We hope our Marginal Gains series has given you some guidance on what to think about in these areas and how to harness the technology available to you.

Want to learn more? Chat to a payments expert ›