stripe

Introduction to online payments

Introduction

This guide covers the basics of online payments and explains the differences for common business models: online retailers, SaaS and subscription companies, and platforms and marketplaces. Start by reading about payment fundamentals and what all businesses need to know about online payments, and then go directly to the section about your business model.

We've also put together a list of the most common industry terms and their definitions, so if you're unfamiliar with any phrases in this guide, refer to the glossary.

> If you want to start accepting online payments right away, read our docs to get started.

Payments fundamentals

Before diving into payment details for different business models, it's helpful to have a high-level understanding of how payments work: how money moves from a customer to your business, how banks facilitate these payments, and the costs involved in the system. Learning about these fundamental building blocks of online payments will help you better understand the nuances of the payments setup for your own business model.

Online payments flow

There are four major players involved in each online transaction:

1. **Cardholder:** The person who owns a credit card
2. **Merchant:** The business owner
3. **Acquirer:** A bank that processes credit card payments on behalf of the merchant and routes them through the card networks (such as Visa or Mastercard) to the issuing bank. Sometimes acquirers may also partner with a third party to help process payments.
4. **Issuing bank:** The bank that extends credit and issues cards to consumers.

To accept online card payments, you need to work with each one of these players (either via a single payments provider or by building your own integrations).

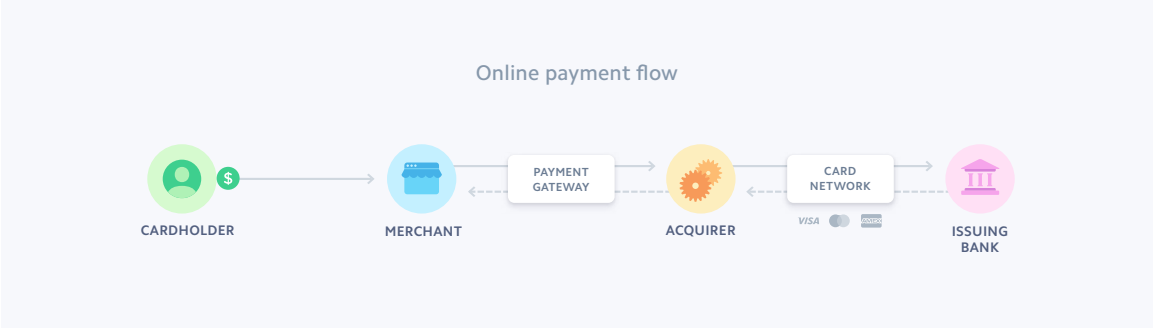
First, you'll need to set up a business bank account and establish a relationship with an acquirer or payment processor. Acquirers and processors help route payments from your website to card networks, such as Visa and Mastercard. Depending on your setup, you may have a separate

acquirer (often a bank that maintains network relationships) and processor (which partners with the acquirer to facilitate transactions), or a single relationship that includes both services.

In order to securely capture payment details, you may also need a gateway, which helps properly secure information. Gateways frequently use tokenization to anonymize payment details and keep sensitive data out of your systems, helping you meet industry-wide security guidelines called PCI standards.

A single provider can offer gateway, processing, and acquiring services, which can help streamline your online payments. Sometimes, the payments provider will build direct integrations with the card networks, helping to reduce third-party dependencies.

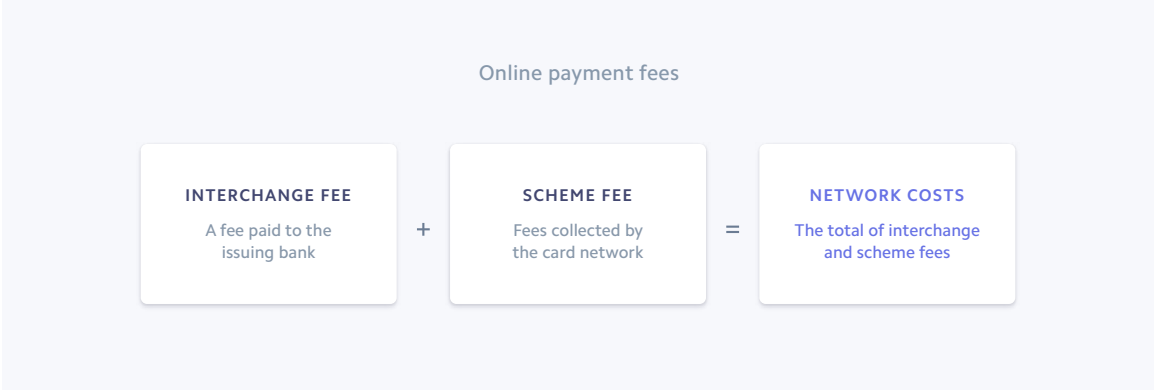
When you accept a payment online, the gateway will securely encrypt the data to be sent to the acquirer, and then to the card networks. The card networks then communicate with the issuing bank, which either confirms or denies the payment (bank rules or regulatory requirements may sometimes require additional card authentication, like 3D Secure, before accepting a payment). The issuing bank will relay the message back to the gateway or acquirer so you can confirm the payment with the customer (by displaying a "payment accepted" or "payment declined" message on your site, for example).



This describes the online payment flow for one-time payments using U.S. dollars in the U.S. If you want to expand internationally, you may need to find a bank partner and set up relationships locally. Or, if you introduce a new product and want to start charging customers on a recurring basis, you would need to not only accept the credit card number, but also accurately initiate and collect payments at a set time interval. You would also need to build logic to accommodate different pricing models, figure out how to recover failed payments, manage prorations when customers switch plans, and more.

Costs involved in online payments

There are a variety of fees that accompany each transaction processed through this four-party system. Visa, Mastercard and other card networks set the fees, referred to as interchange and scheme fees.



Interchange typically represents the bulk of the costs involved in a transaction. This amount is given to the issuing bank because it takes on the greatest amount of risk by extending credit or banking services to the cardholder.

Scheme fees are collected by the card networks themselves and can include additional authorization and cross-border transaction fees. Fees can also be assessed for refunds and other network services.

Together, these fees make up the network costs. These vary depending on the card type, transaction location, channel (in-person or online), and Merchant Category Code (MCC). For example, a transaction made with a rewards credit card would incur higher network fees than a transaction with a non-rewards card since banks often use these fees to subsidize the cost of the rewards program.

Stripe's standard pay-as-you-go pricing offers a single, transparent rate for all card payments, helping give you more predictability over your payment costs. Learn more.

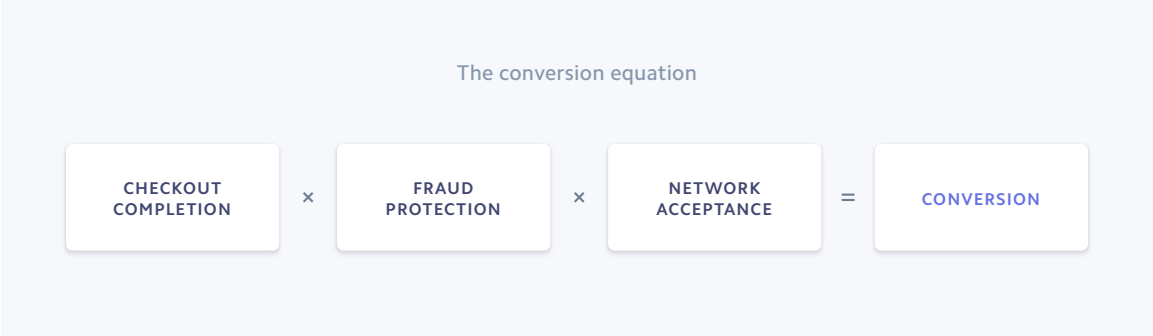
For all businesses accepting online payments

This section covers two important topics for all businesses accepting payments: how the online payments funnel can increase your conversion, and how adding the right payment methods can expand your pool of potential customers.

Online payments funnel

Transactions go through three steps to make a purchase: checkout completion, fraud protection, and network acceptance. Conversion happens when a transaction is successfully completed.

Through each stage of the funnel, your pool of potential customers can gradually shrink. If you have a long or complicated checkout process, a fraction of customers will fall off. Then, when you factor in fraud and average transaction acceptance rates, the pool shrinks even more.



Understanding the interaction between these steps is important to optimizing your entire funnel. This is especially true for businesses that have separate teams owning checkout, fraud, and network acceptance, with each one optimizing for their own metrics. For example, if the team working on checkout completion solely focuses on reducing cart abandonment rates, they may ask for less customer information to reduce friction. However, this can result in more fraud since you're not always capturing details like the full billing address and ZIP code to help validate the transaction.

In this section, we'll give you an overview of the online payments funnel and share best practices to increase conversion.

Designing the best checkout forms

The online payments funnel starts with the checkout experience, where customers enter their payment information to purchase goods or services. At this stage, you want to collect enough details to be able to verify that customers are who they say they are, but avoid adding too much friction to the checkout process—which can cause customers to abandon it altogether.

If your checkout form is too complicated, you risk losing sales from the most likely buyers—customers with items in their cart and every intention to make a purchase. In fact, 87% of customers abandon a purchase if the checkout process is too difficult.

To improve your checkout completion rate, the first step is to go through your own checkout process from the customer's point of view and look for any friction that could lead to drop off. Pay attention to how long the site takes to load, how many fields are in your form, and if your checkout process supports autofill.

The best checkout forms adapt to the customer's experience. For example, it's best practice to offer responsive checkout forms that automatically resize to the smaller screen of a mobile device and offer a numerical keypad when customers are prompted to enter their card information. You should also consider supporting mobile wallets, such as Apple Pay or Google Pay, to bypass manual data entry.

If you choose to expand internationally, your checkout form should cater to each market. Allowing customers to pay in their local currency is a start, but you also need to support local payment

methods to provide the most relevant experience. For example, more than half of customers in the Netherlands prefer to pay with iDEAL, a payment method which directly transfers funds from a customer's bank account to the business.

The card number can also indicate where a customer is located geographically, allowing you to dynamically change the form fields to capture the right information for each country. For example, if your form recognizes a U.K. card, you should add a field to capture the postcode. If your form recognizes an American card, you should change that field to ZIP code.

Stripe Checkout is a drop-in payments page designed to drive conversion. It dynamically surfaces mobile wallets when appropriate and supports 15 languages so customers can use a checkout form that's personalized and relevant. Learn more.

Managing risk online

The next step is to evaluate whether a transaction is fraudulent. The majority of illegitimate payments involve fraudsters pretending to be legitimate customers by using stolen cards and card numbers.

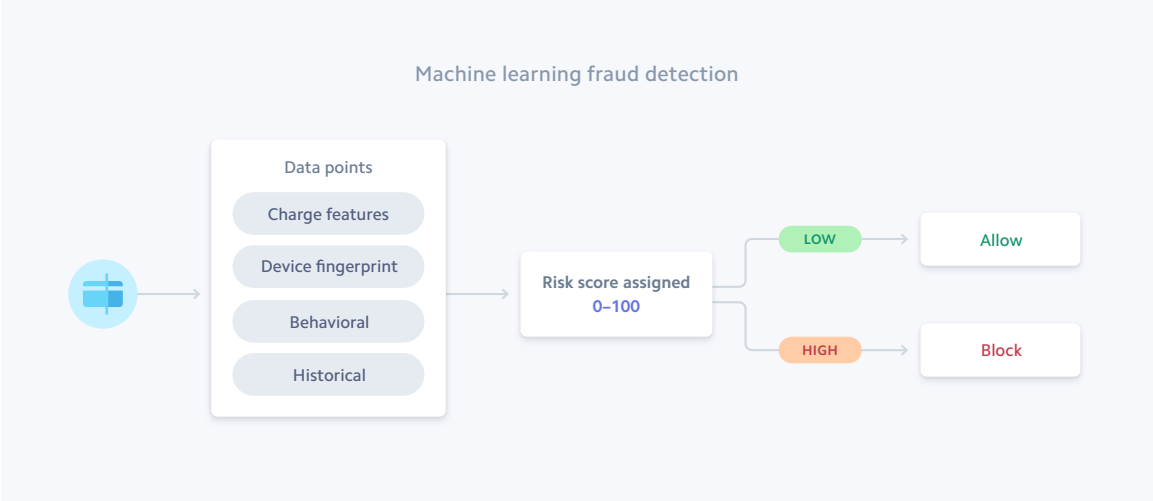
For example, if a fraudster makes a purchase on your website using a stolen card number that hasn't been reported, it's possible the payment would be processed successfully. Then, when the cardholder discovers the fraudulent use of the card, he or she would question the payment with his or her bank by filing a chargeback. While you have the chance to dispute this chargeback by submitting evidence about whether the payment was valid, card network rules tend to favor the customer in most disputes. If your business loses a dispute, your business would lose the original transaction amount. You, as the business owner, would also have to pay a chargeback fee, the cost associated with the bank reversing the card payment.

While chargebacks are a part of accepting payments online, the best way to manage them is to prevent them from happening in the first place. There are two primary approaches: rules-based logic and machine learning.

Rules-based fraud detection operates on an "If x happens, then do y" logic created and is managed on an ongoing basis by fraud analysts. Examples include blocking all transactions from a certain country, IP address, or above a certain dollar amount. However, because this logic is based on strict rules, it doesn't recognize hidden patterns nor does it adapt to shifting fraud vectors by analyzing information beyond these defined parameters. As a result, analysts are often playing catch up—manually creating new rules after they detect fraud rather than proactively fighting fraud.

Fraud management based on machine learning, on the other hand, can use transaction data to train algorithms that learn and adapt. Some machine learning models mimic the behavior of human reviewers, while others are trained by millions of data points. These models learn how to

discern legitimate transactions from those that are potentially fraudulent. Some of these models can even train themselves, making them more scalable and efficient than rules-based logic.



For example, let's say a customer with normal browsing behavior and a suspicious IP address wants to purchase something from your site. Machine learning decides how much weight each of these signals should carry. For example, should the transaction be declined solely based on the IP address? A rules-based system may block all transactions from that location, but a machine learning model should be able to distinguish between good and bad transactions from by weighting the location alongside all the other information available to determine the probability that a given payment will result in a chargeback.

Combining these two approaches—rules-based logic and machine learning fraud management—can be a powerful, customizable solution. You are able to leverage the sophistication of machine learning, but also customize the approach and encode logic that is specific to your business. For example, you can set custom rules based on the risk level of a subset of your users and what they are buying.

For more information, read our guide on machine learning for fraud detection.

Stripe Radar is a suite of modern tools for fraud detection and prevention. Its core is powered by adaptive machine learning, with algorithms evaluating every transaction for fraud risk and taking appropriate actions. Radar is included for free as part of Stripe's integrated pricing. Users can upgrade to Radar for Fraud Teams to set their own rules-based logic, and use other powerful tools for fraud professionals.

Improving network acceptance

The last step in the online payments funnel is card network acceptance: having the issuing bank successfully process the payment.

When customers make a purchase, a payment request is sent to the issuing bank. Based on a variety of factors, ranging from your customer's available balance, the formatting of transaction metadata, or even system downtime, the issuing bank will either accept or decline the request. The higher your acceptance rate, the more transactions you've been able to successfully process.

You can help reduce unnecessary declines by collecting additional data or passing through details like CVC, billing address, and ZIP code during checkout. This information gives the issuing bank extra information about the transaction, helping improve the chances of acceptance for legitimate transactions.

> Stripe helps automatically improve network acceptance for businesses thanks to direct network integrations and industry partnerships that provide additional data and insights into the reasons for declines. We use this to build machine learning models that identify the best ways to update payment metadata to improve the chances of acceptance. Learn more.

Global payment methods

While cards are the predominant online payment method in the U.S., 40% of consumers outside the U.S. prefer to use a payment method other than a credit card, including bank transfers and digital wallets (such as Alipay, WeChat Pay, or Apple Pay). You may lose sales simply because you don't offer the preferred payment methods of a global audience.

To capitalize on a global customer base, you need to offer the payment methods that are most commonly used in the countries in which you operate. There are the five common types of payment methods:

1. **Credit cards** allow customers to borrow funds from a bank and either pay the balance in full each month or pay the money back with interest. **Debit cards** make payments by deducting money directly from a customer's checking account, rather than using a line of credit.
2. **Digital wallets**, including Apple Pay and Google Pay, let customers pay for products or services electronically by linking a card or bank account. Digital wallets can also allow customers to store monetary value directly in the app with top-ups.
3. **Bank debits and transfers** move money directly from a customer's bank account. Account debits collect your customers' banking information and pull funds from their accounts (for example, ACH in the U.S.). Credit transfers link to customers' bank accounts and they push

money to you (like wire transfers). There are also payment methods like Giropay in Germany and iDEAL in the Netherlands that operate as a layer on top of banks to facilitate transfers, but look more like digital wallets.

4. **Buy now, pay later** is a growing category of payment methods that offers customers immediate financing for online payments, typically repaid in fixed installments over time. Examples include Afterpay, Klarna, and Affirm.

5. **Cash-based payment methods,** from companies like OXXO and Boleto, allow customers to make online purchases without a bank account. Instead of paying for a product or service, customers receive a scannable voucher with a transaction reference number that they can then bring to an ATM, bank, convenience store, or supermarket and make a payment in cash. Once the reference number for the cash payment is matched to the initial purchase, the business gets paid and can ship the product.

For more information, read our guide to payment methods.

Stripe lets you support dozens of payment methods with a single integration. Learn more.

Online retailers

Read this section if you want to sell goods in-person at retail locations in addition to your website or mobile app.

Increasingly, retailers that started as online-only operations are finding success in expanding into the physical world by opening in-person locations. With more than 90% of purchases still happening in person, this creates the potential for digital businesses to create a new revenue stream.

The challenge, however, is unifying data across your online and in-person payments. Customers expect to engage with your business in the same way across channels and, as part of that, how they make a purchase needs to be consistent and on-brand. For example, users may expect discount codes and promotions to apply to both online and in-person purchases.

Here are two things you need to know if you want to expand your online business to support in-person sales:

1. **Leverage existing infrastructure**

   Retailers often have to set up two seperate payment providers: one for online and one for in-person purchases. This requires two integrations and two separate accounts, doubling the amount of work required to get started, making it hard to manage financial reconciliation, and often siloing customer data within each account.

Instead, make sure you leverage your existing payments infrastructure—what you already set up for online payments—rather than onboarding a new vendor. This not only saves you time and resources, it also simplifies reporting and helps create a more unified customer experience.

This creates a seamless payments experience whether customers make a purchase on their smartphone or walk into your store. For example, customers could start a subscription in person that continues online. The payment method they used in the store would be saved to their online profile, where they would be able to update any details or change the subscription cadence.

2 Support chip cards and mobile wallets

Magnetic stripe cards increase a business's exposure to risk because they're easy for fraudsters to copy and require additional steps to encrypt customer payment information. As a result, EMV chip cards—which are more secure and protect businesses from liability in the event of fraud—have been the global standard for decades.

In 2015, the U.S. began its transition to chip cards and today, they are used for the majority of credit card transactions. However, there are still businesses that use older card readers that support magnetic stripe cards. As you're evaluating hardware to accept in-person payments, it's important to pick a newer card reader that allows you to accept chip cards.

You should also consider supporting mobile wallets, such as Apple Pay and Google Pay, for in-person transactions. Like chip cards, they securely encrypt payment information and minimize your liability associated with fraudulent transactions. Mobile wallets also improve the payment experience, making transactions more convenient and streamlined for customers.

Stripe Terminal helps you unify your online and offline channels with flexible developer tools, pre-certified card readers, and cloud-based hardware management.

SaaS and subscription companies

Read this section if you charge your customers on a recurring basis or use stored payment information.

When managing recurring revenue, there's a lot of complexity around how you initiate and collect payments, and accommodate different pricing models. You must store customers' payment information and accurately charge them at set time intervals.

There are two ways to set this up: build your own payments system or buy existing software. Either way, you need to make sure your billing system can accept orders from a web or mobile checkout, correctly bill the customer based on the pricing model (flat-rate billing or tiered pricing, for example), and collect payments using whichever payment methods customers prefer to use. You also need the ability to surface insights that are important for recurring businesses, including churn, monthly recurring revenue, and other key subscription metrics—or integrate with your customer relationship management system or account system.

As you decide whether to build your own software from scratch or buy an existing one, think about the opportunity costs. Consider the ongoing engineering resources required to build and maintain your billing software versus the other needs of your business.

Here are three considerations for SaaS and subscription payments:

1. **Set flexible subscription logic**

   Subscription logic is made up of time-based and price-based rules that, together, accurately charge your customers on a predetermined cadence. When you only have one product and simple pricing, like $25 per month for a software subscription, setting up this logic in your billing system is easy because the dollar amount doesn't change from month to month.

   Over time, you may expand your business to add new products and promotions. You need to ensure that your subscription logic can handle this growth with the ability to experiment with different pricing models, like flat-rate, per-seat, or metered subscriptions, tiered pricing, freemium, and free trials. You may also want the ability to offer bundles or discounts.

   Your subscription logic should also be flexible enough to account for customers changing plans at any time. If someone wants to switch to a cheaper plan mid-month, you have to prorate the costs of both plans and ensure that the customer will be charged for the right amount going forward.

2. **Think about your invoicing needs**

   Customers usually prefer to receive an invoice if you're charging them for a large amount or sending a one-off bill (both of which are common for SaaS companies that have other businesses as their customers).

   To send invoices, think about what the creation process should look like: do invoices have the same line items or does each one need to be customized? Depending on which countries you are operating in, you also have to follow different invoice requirements. For example, you may have to follow sequential invoice numbering or set invoice prefixes at either the customer or account level.

   Then, you need a way to send the invoices to your customers. Think about whether you want to manually send them via email or if your billing solution can automate this process for you.

3 Minimize involuntary churn

Most SaaS and subscription companies face involuntary churn issues, where customers intend to pay for a product but their payment attempt fails due to expired cards, insufficient funds, or outdated card details (9% of subscription invoices fail on the first charge attempt due to involuntary churn).

When you only have a handful of failed payments a month, it's easy to call or email each customer and ask him or her to remedy the situation (whether that's by using a new payment method or updating payment information). However, as your business grows and you have to manage hundreds of customers with failed payments, this approach becomes less manageable.

A more scalable way to communicate with your customers is to send automated failed payment emails whenever a payment is declined.

In addition to outbound communication, you can also retry payments directly. Many businesses will retry failed transactions on a set schedule, like every seven days (this process is known as dunning). Experiment with different cadences to learn what is most effective for your business or find a payments provider that automates the dunning process and allows you to adapt it based on your customers' preferences.

Stripe Billing offers an end-to-end billing solution. You can create and manage subscription logic and invoices, accept any supported payment method, and reduce involuntary churn with smart retry logic.

Platforms and marketplaces

Read this section if you are a software platform and enable other businesses to accept payments directly from their customers (like Shopify) or if you are a marketplace, where you collect payments from customers and then pay them out to sellers or service providers (like Lyft).

Platforms and marketplaces have some of the most complex payment requirements because they accept money on behalf of sellers or service providers and issue payouts to them. As a result, there are many unique considerations, including verifying sellers' identities, compliantly managing money transmission, taking a service fee from each payment, and filing 1099s with the IRS when applicable.

However, providing payments functionality to your customers allows you to differentiate your platform or marketplace and add value for your sellers or service providers. You can help them launch businesses faster without having to worry about lengthy merchant account applications or writing code to be able to accept payments.

Traditionally, adding payments functionality required you to become licensed, and register and maintain status as a payment facilitator with card networks (such as Visa or Mastercard). Since you are seen as controlling the flow of funds when you move money between buyers and sellers, the card networks apply strict regulations. This process can take months (sometimes years) and require millions of dollars in upfront and ongoing costs.

Today, however, several options exist for platforms and marketplaces to add customized payments capabilities for their customers and earn revenue from payments, without having to register as a payment facilitator themselves.

Here are two capabilities you need to consider when adding payments to your platform or marketplace:

1. Verify users during onboarding

   Before you accept any money on behalf of your sellers or businesses, you need to onboard them to your payment system and verify their identity. This step is complicated due to stringent laws and regulations including Know Your Customer (KYC) laws and sanctions screening requirements, which carry penalties and fines for violations. In addition to government regulations, which can vary from country to country, card networks including Visa and Mastercard have their own information collection requirements, which are regularly updated.

   Balancing these information requirements with the user experience is delicate. On the one hand, you want to collect as much information as possible (such as full name, email, date of birth, last four digits of their social security number in the U.S., phone number, and address) to ensure your platform isn't being used for nefarious purposes like money laundering or terrorist financing. You also want to avoid penalties with regulatory bodies and financial partners.

   On the other hand, you want to make your user experience better than the competition. That means providing a low-friction onboarding experience, which isn't always compatible with detailed information requests.

   To help remove friction, consider collecting data in a phased approach and auto-completing fields for your users when possible. For example, you could only ask for sellers' or service providers' tax information once they pass an IRS reporting threshold. And, you could pre-populate fields for their legal name and address if you already collected this information.

2. Support different ways to move money

   Paying your users involves more than just moving money from point A to point B. You need the ability to collect service fees for your platform, split and route funds among sellers, and control when payouts are sent to your sellers' bank accounts.

Let's say you run an e-commerce platform and a customer makes a $50 purchase from a seller. You need to think about three parties: your platform, your sellers or service providers, and their buyers or end-users. Before you pay the seller, you need to take your platform fee. Then, you need to figure out how and when to send the remaining funds to the seller. Do you send the payout immediately upon receipt of the goods or services, or do you aggregate the funds and pay out every week? Do you have the correct banking information to route the payment?

You also need to ensure you're moving money in a compliant way. For example, in the U.S., 46 states require their own licenses to move money on behalf of others. In Europe, PSD2 laws require licensing for payment intermediaries. If you are deemed a money transmitter or payment intermediary by a regulatory body and are not licensed, you can be fined or at risk of being shut down.

Depending on your business model, you should be able to support a number of different ways of moving money, such as:

- **One-to-one:** One customer is charged and one recipient is paid out (e.g. a ride-sharing service).
- **One-to-many:** One transaction is split between multiple sellers or recipients (e.g. a retail marketplace where a customer purchases one "cart" with items sourced from multiple online stores).
- **Holding funds:** A platform accepts funds from customers and holds them in reserve before paying out recipients (e.g. a ticketing platform that pays recipients only after an event has taken place).
- **Account debits:** A platform performs a debit or transaction reversal to pull funds from its sellers or service providers (e.g. an e-commerce platform pulling a monthly store maintenance fee from its business customers).
- **Subscriptions:** A platform allows its sellers to collect a recurring charge from customers (e.g. a SaaS platform enables its nonprofits to accept recurring donations).

Stripe Connect enables platforms and marketplaces to facilitate payments for their sellers, service providers, and customers. It supports onboarding and verification, allows you to accept 135+ currencies and dozens of local payment methods around the world with built-in fraud protection, pay out users, and track the flow of funds

Additional reading

We hope this guide gave you a high-level overview of online payments and helped you understand the nuances of your own payments setup.

This is our first guide in a series about the fundamentals of online payments. We'll continue to explore foundational concepts, like in-person and recurring payments, as well as more advanced topics like declines and payout management, in future guides.

In the meantime, here is some additional reading:

All businesses accepting payments

- A guide to payment methods
- A guide to PCI compliance
- A primer on machine learning for fraud detection
- 3D Secure 2: A new authentication standard

Online retailers

- How to use Stripe Terminal to accept in-person payments

SaaS companies

- How to create and charge for a subscription with Stripe
- A guide to SaaS businesses and how to grow them
- SCA best practices for recurring revenue businesses

Platforms and marketplaces

- How to route payments between multiple parties with Stripe
- How PSD2 impacts marketplaces and platforms in Europe
- A guide to payment facilitation for platforms and marketplaces

Payments glossary

This glossary defines the most common terms in the payments industry.

Acquirer

Also referred to as an acquiring bank, an acquirer is a bank or financial institution that processes credit or debit card payments on behalf of the merchant and routes them through the card networks to the issuing bank.

Bank transfers

Can refer to an account debit, where you collect your customers' banking information and pull funds from their accounts, or a credit transfer, where you link to customers' bank accounts and they push money to you.

Cardholder

A person who owns a credit or debit card.

Card networks

Process transactions between merchants and issuers and control where credit cards can be accepted. They also control the network costs. Examples include Visa, Mastercard, and American Express.

Chargeback

Also referred to as a dispute, a chargeback occurs when cardholders question a payment with their card issuer. During the chargeback process, the burden is on the merchant to prove that the person who made the purchase owns the card and authorized the transaction.

Chargeback fees

The cost incurred by the merchant when the acquiring bank reverses a card payment.

Digital wallet

Lets customers pay for products or services electronically by linking a card or bank account, or storing monetary value directly in the app. Examples include Apple Pay, Google Pay, Alipay, and WeChat.

Disputes

See definition for "Chargeback"

Four-party system

The four parties involved in processing payments: the cardholder, merchant, acquirer, and issuing bank.

Fraud

Any false or illegal transaction. It typically occurs when someone has stolen a card number or checking account data and uses that information to make an unauthorized transaction.

Interchange

A fee paid to the issuing bank for processing a card payment.

Issuing bank

The bank that issues credit and debit cards to consumers on behalf of the card networks.

Merchant Category Code (MCC)

A four-digit number used to classify a business by the type of goods or services it provides.

Network acceptance

The percentage of transactions that are accepted or declined by the issuing bank. A decline can occur due to outdated credentials, suspicion of fraud, or insufficient funds.

Network costs

The total of interchange and scheme fees.

Payment facilitator

Traditionally, adding payments functionality required a platform or marketplace to register and maintain status as a payment facilitator (or payfac) with the card networks, since it was seen as controlling the flow of funds between buyers and sellers. Today, it's easy to add the payments functionality that most platforms and marketplaces require without becoming a payment facilitator.

Payment gateway

A piece of software that encrypts credit card information on a merchant's server and sends it to the acquirer. Gateway services and acquirers are often the same entity.

Payment method

The way a consumer chooses to pay for goods or services. Payment methods include bank transfers, credit or debit cards, and digital wallets.

Payment processor

Facilitates the credit card transaction by sending payment information between the merchant, the issuing bank, and the acquirer. The payment processor usually gets the payment details from a payment gateway.

PCI Data Security Standards (PCI DSS)

An information security standard that applies to all entities involved in storing, processing, or transmitting cardholder data, and/or sensitive authentication data.

Scheme fees

Fees collected by the card network. A single transaction may incur multiple scheme fees, such as authorization fees or service fees.