



Privacy Policy

Last updated: January 16, 2025

This Privacy Policy includes important information about your personal data and we encourage you to read it carefully.

Welcome

We provide financial infrastructure for the internet. Individuals and businesses of all sizes use our technology and services to facilitate purchases, accept payments, send payouts, and manage online businesses.

This Privacy Policy ("Policy") describes the Personal Data that we collect, how we use and share it, and details on how you can reach us with privacy-related inquiries. The Policy also outlines your rights and choices as a data subject, including the right to object to certain uses of your Personal Data.

Depending on the activity, Stripe assumes the role of a "data controller" and/or "data processor" (or "service provider"). For more details about our privacy practices, including our role, the specific Stripe entity responsible under this Policy, and our legal bases for processing your Personal Data, please visit our [Privacy Center](#).

Defined Terms

In this Policy, "Stripe", "we", "our," or "us" refers to the Stripe entity responsible for the collection, use, and handling of Personal Data as described in this document. Depending on your jurisdiction, the specific Stripe entity accountable for your Personal Data might vary. [Learn More](#).

"Personal Data" refers to any information associated with an identified or identifiable individual, which can include data that you provide to us, and that we collect about you during your interaction with our Services (such as device information, IP address, etc.).

"Services" refers to the products, services, devices, and applications, that we provide under the Stripe Services Agreement ("Business Services") or the Stripe Consumer Terms of Service ("End User Services"); websites ("Sites") like Stripe.com and Link.com; and other Stripe applications and online services. We provide Business Services to entities ("Business Users"). We provide End User Services directly to individuals for their personal use.

"Financial Partners" are financial institutions, banks, and other partners such as payment method acquirers, payout providers, and card networks that we partner with to provide the Services.

Depending on the context, "you" might be an End Customer, End User, Representative, or Visitor:

End Users. When you use an End User Service, such as saving a payment method with Link, for personal use we refer to you as an “End User.”

End Customers. When you are not directly transacting with Stripe, but we receive your Personal Data to provide Services to a Business User, including when you make a purchase from a Business User on a Stripe Checkout page or receive payments from a Business User, we refer to you as an “End Customer.”

Representatives. When you are acting on behalf of an existing or potential Business User—perhaps as a company founder, account administrator for a Business User, or a recipient of an employee credit card from a Business User via Stripe Issuing—we refer to you as a “Representative.”

Visitors. When you interact with Stripe by visiting a Site without being logged into a Stripe account, or when your interaction with Stripe does not involve you being an End User, End Customer, or Representative, we refer to you as a “Visitor.” For example, you are a Visitor when you send a message to Stripe asking for more information about our Services.

In this Policy, “Transaction Data” refers to data collected and used by Stripe to facilitate transactions you request. Some Transaction Data is Personal Data and may include: your name, email address, contact number, billing and shipping address, payment method information (like credit or debit card number, bank account details, or payment card image chosen by you), merchant and location details, amount and date of purchase, and in some instances, information about what was purchased.

1. Personal Data that we collect and how we use and share it

2. More ways we collect, use and share Personal Data

3. Legal bases for processing data

4. Your rights and choices

5. Security and retention

6. International data transfers

7. Updates and notifications

8. Jurisdiction-specific provisions

9. Contact us

10. US Consumer Privacy Notice

1. Personal Data we collect and how we use and share it

Our collection and use of Personal Data differs based on whether you are an End User, End Customer, Representative, or Visitor, and the specific Service that you are using. For example, if you're a sole proprietor who wants to use our Business Services, we may collect your Personal Data to onboard your business; at the same time, you might also be an End Customer if you've bought goods from another Business User that is using our Services for payment processing. You could also be an End User if you used our End User Service, such as Link, for those transactions.

1.1 End Users

We provide End User Services when we provide the Services directly to you for your personal use (e.g., Link). Additional details regarding our collection, usage, and sharing of End User Personal Data, including the legal bases we rely on for processing such data, can be found in our [Privacy Center](#).

a. Personal Data we collect about End Users

Using Link or Connecting your bank account. Stripe offers a service called "Link," which allows you to create an account and store information for future interactions with Stripe's Services and Business Users. You may save a number of different kinds of Personal Data using Link. For instance, you may save your name, payment method details, contact information, and address to conveniently use saved information to pay for transactions across our Business Users. When you choose to pay with Link, we will also collect Transaction Data associated with your transactions. [Learn More](#).

You can also share and save bank account details to your Link account using Stripe's **Financial Connections** product. When you use Financial Connections, Stripe will periodically collect and process your account information (such as bank account owner information, account balances, account number and details, account transactions, and, in some cases, log-in credentials). You can ask us to cease the collection of such data at any time. [Learn More](#).

Finally, you can use Link to store your identity documents (such as your driver's license) so that you can share them in future interactions with Stripe or its Business Users.

Paying Stripe. When you purchase goods or services directly from Stripe, we receive your Transaction Data. For instance, when you make a payment to Stripe Climate, we collect information about the transaction, as well as your contact and payment method details.

Identity/Verification Services. We offer an identity verification service that automates the comparison of your identity document (such as a driver's license) with your image (such as a selfie). You can separately consent to us using your biometric data to enhance our verification technology, with the option to revoke your consent at any time. [Learn More](#).

More. For further information about other types of Personal Data that we may collect about End Users, including about your online activity and your engagement with our End User Services, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Personal Data of End Users

Services. We use and share your Personal Data to provide the End User Services to you, which includes support, personalization (such as language preferences and setting choices), and communication about our End User Services (such as communicating Policy updates and information about our Services). For example, Stripe may use cookies and similar technologies or the data you provide to our Business Users (such as when you input your email address on a Business User's website) to recognize you and help you use Link when visiting our Business User's website. Learn more about how we use cookies and similar technologies in Stripe's [Cookie Policy](#).

Our Business Users. When you use Link to make payments with our Business Users, we share your Personal Data, including name, contact information, payment method details, and Transaction Data with those Business Users. [Learn More](#). You can also direct Stripe to share your saved bank account information and identity documents with Business Users you do business with. Once we share your Personal Data with Business Users, we may process that Personal Data as a Data Processor for those Business Users, as detailed in Section 1.2 of this Policy. You should consult the privacy policies of the Business Users' you do business with for information on how they use the information shared with them.

Fraud Detection and Loss Prevention. We use your Personal Data collected across our Services to detect fraud and prevent financial losses for you, us, and our Business Users and Financial Partners, including detecting unauthorized purchases. We may provide Business Users and Financial Partners, including those that use our fraud prevention-related Business Services (such as Stripe Radar), with Personal Data about you (including your attempted transactions) so that they can assess the fraud or loss risk associated with the transaction. Learn more about how we may use technology to assess the fraud risk associated with an attempted transaction and what information we share with Business Users and Financial Partners [here](#) and [here](#).

Advertising. Where permitted by applicable law, we may use your Personal Data, including Transaction Data, to assess your eligibility for, and offer you, other End User Services or promote existing End User Services, including through co-marketing with partners such as Stripe Business Users. **Learn more.** Subject to applicable law, including any consent requirements, we use and share End User Personal Data with third party partners to allow us to advertise our End User Services to you, including through interest-based advertising, and to track the efficacy of such ads. We do not transfer your Personal Data to third parties in exchange for payment, but we may provide your data to third-party partners, such as advertising partners, analytics providers, and social networks, who assist us in advertising our Services to you. **Learn more.**

More. For further information about ways we may use and share End Users' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

1.2 End Customers

Stripe provides various Business Services to our Business Users, which include processing in-person or online payments or payouts for those Business Users. When acting as a service provider—also referred to as a Data Processor—for a Business User, we process End Customer Personal Data in accordance with our agreement with the Business User and the Business User's lawful instructions. This happens, for example, when we process a payment for a Business User because you purchased a product from them, or when the Business User asks us to send you funds.

Business Users are responsible for ensuring that the privacy rights of their End Customers are respected, including obtaining appropriate consents and making disclosures about their own data collection and use associated with their products and services. If you're an End Customer, please refer to the privacy policy of the Business User you're doing business with for its privacy practices, choices, and controls.

We provide more comprehensive information about our collection, use, and sharing of End Customer Personal Data in our [Privacy Center](#), including the [legal bases](#) we rely on for processing your Personal Data.

a. Personal Data we collect about End Customers

Transaction Data. If you're an End Customer making payments to, receiving refunds or payments from, initiating a purchase or donation, or otherwise transacting with our Business User, whether in-person or online, we receive your Transaction Data. We may also receive your transaction history with the Business User. **Learn More.** Additionally, we may collect information entered into a checkout form even if you opt not to complete the form or transaction with the Business User. **Learn More.** A Business User who uses Stripe's Terminal Service to provide its goods or services to End Customers may use the Terminal Service to collect End Customer Personal Data (like your name, email, phone number, address, signature, or age) in accordance with its own privacy policy.

Identity/Verification Information. Stripe provides a verification and fraud prevention Service that our Business Users can use to verify Personal Data about you, such as your authorization to use a particular payment method. During the process, you'd be asked to share with us certain Personal Data (like your government ID and selfie for biometric verification, Personal Data you input, or Personal Data that is apparent from the physical payment method like a credit card image). To protect against fraud and determine if somebody is trying to impersonate you, we may cross-verify this data with information about you that we've collected from Business Users, Financial Partners, business affiliates, identity verification services, publicly available sources, and other third party service providers and sources. **Learn More.**

More. For further information about other types of Personal Data that we may collect about End Customers, including about your online activity, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Personal Data of End Customers

To provide our Business Services to our Business Users, we use and share End Customers' Personal Data with them. Where allowed, we also use End Customers' Personal Data for Stripe's own purposes such as enhancing security, improving and offering our Business Services, and preventing fraud, loss, and other damages, as described further below.

Payment processing and accounting. We use your Transaction Data to deliver Payment-related Business Services to Business Users — including online payment transactions processing, sales tax calculation, and invoice, bill, and dispute handling — and to help them determine their revenue, settle their bills, and execute accounting tasks. **Learn More.** We may also use your Personal Data to provide and improve our Business Services.

During payment transactions, your Personal Data is shared with various entities in connection with your transaction. As a service provider or data processor, we share Personal Data to enable transactions as directed by Business Users. For instance, when you choose a payment method for your transaction, we may share your Transaction Data with your bank or other payment method provider, including as necessary to authenticate you, **Learn More**, process your transaction, prevent fraud, and handle disputes. The Business User you choose to do business with also receives Transaction Data and might share the data with others. Please review your merchant's, bank's, and payment method provider's privacy policies for more information about how they use and share your Personal Data.

Financial services. Certain Business Users leverage our Services to offer financial services to you via Stripe or our Financial Partners. For example, a Business User may issue a card product with which you can purchase goods and services. Such cards could carry the brand of Stripe, the bank partner, and/or the Business User. In addition to any Transaction Data we may generate or receive when these cards are used for purchases, we also collect and use your Personal Data to provide and manage these products, including assisting our Business Users in preventing misuse of the cards. Please review the privacy policies of the Business User and, if applicable, our bank partners associated with the financial service (the brands of which may be shown on the card) for more information.

Identity/Verification services. We use Personal Data about your identity to perform verification services for Stripe or for the Business Users that you are transacting with, to prevent fraud, and to enhance security. For these purposes we may use Personal Data you provide directly or Personal Data we obtain from our service providers, including for phone verification. **Learn More.** If you provide a selfie along with an image of your identity document, we may employ biometric technology to compare and calculate whether they match and verify your identity. **Learn More.**

Fraud detection and loss prevention. We use your Personal Data collected across our Services to detect and prevent losses for you, us, our Business Users, and Financial Partners. We may provide Business Users and Financial Partners, including those using our fraud prevention-related Business Services, with your Personal Data (including your attempted transactions) to help them assess the fraud or loss risk associated with a transaction. Learn more about how we may use technology to assess the fraud risk associated with an attempted transaction and what information we share with Business Users and Financial Partners [here](#) and [here](#).

Our Business Users (and their authorized third parties). We share End Customers' Personal Data with their respective Business Users and parties directly authorized by those Business Users to receive such data. Here are common examples of such sharing:

When a Business User instructs Stripe to provide another Business User with access to its Stripe account, including data related to its End Customers, via Stripe Connect.

Sharing information that you have provided to us with a Business User so that we can send payments to you on behalf of that Business User.

Sharing information, documents, or images provided by an End Customer with a Business User when the latter uses Stripe Identity, our identity verification Service, to verify the identity of the End Customer.

The Business Users you choose to do business with may further share your Personal Data with third parties (like additional third party service providers other than Stripe). Please review the Business User's privacy policy for more information.

Advertising by Business Users. If you initiate a purchasing process with a Business User, the Business User receives your Personal Data from us in connection with our provision of Services even if you don't finish your purchase. The Business User may use your Personal Data to market and advertise their products or services, subject to the terms of their privacy policy. Please review the Business User's privacy policy for more information, including your rights to stop their use of your Personal Data for marketing purposes.

More. For further information about additional ways by which we may use and share End Customers' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

1.3 Representatives

We collect, use, and share Personal Data from Representatives of Business Users (for example, business owners) to provide our Business Services. For more information about how we collect, use, and share Personal Data from Representatives, as well as the legal bases we rely on for processing such Personal Data, please visit our [Privacy Center](#).

a. Personal Data we collect about Representatives

Registration and contact information. When you register for a Stripe account for a Business User (including incorporation of a Business), we collect your name and login credentials. If you register for or attend an event organized by Stripe or sign up to receive Stripe communications, we collect your registration and profile data. As a Representative, we may collect your Personal Data from third parties, including data providers, to advertise, market, and communicate with you as detailed further in the *More ways we collect, use, and share Personal Data* section below. We may also link a location with you to tailor the Services or information effectively to your needs. [Learn More](#).

Identification Information. As a current or potential Business User, an owner of a Business User, or a shareholder, officer, or director of a Business User, we need your contact details, such as name, postal address, telephone number, and email address, to fulfill our Financial Partner and regulatory requirements, verify your identity, and prevent fraudulent activities and harm to the Stripe platform. We collect your Personal Data, such as ownership interest in the Business User, date of birth, government-issued identity documents, and associated identifiers, as well as any history of fraud or misuse, directly from you and/or from publicly available sources, third parties such as credit bureaus and via the Services we provide. [Learn More](#). You may also choose to provide us with bank account information.

More. For further information about other types of Personal Data that we may collect about Representatives, including your online activity, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Personal Data of Representatives

We typically use the Personal Data of Representatives to provide the Business Services to the corresponding Business Users. The ways we use and share this data are further described below.

Business Services. We use and share Representatives' Personal Data with Business Users to provide the Services requested by you or the Business User you represent.

In some instances, we may have to submit your Personal Data to a government entity to provide our Business Services, for purposes such as the incorporation of a business, or calculating and paying applicable sales tax. For our tax-related Business

Services, we may use your Personal Data to prepare tax documents and file taxes on behalf of the Business User you represent. For our Atlas business incorporation Services, we may use your Personal Data to submit forms to the IRS on your behalf and file documents with other government authorities, such as articles of incorporation in your state of incorporation.

We share Representatives' Personal Data with parties authorized by the corresponding Business User, such as Financial Partners servicing a financial product, or third party apps or services the Business User chooses to use alongside our Business Services. Here are common examples of such sharing:

Payment method providers, like Visa or WeChat Pay, require information about Business Users and their Representatives who accept their payment methods. This information is typically required during the onboarding process or for processing transactions and handling disputes for these Business Users. [Learn More](#).

A Business User may authorize Stripe to share your Personal Data with other Business Users to facilitate the provision of Services through Stripe Connect.

The use of Personal Data by a third party authorized by a Business User is subject to the third party's privacy policy.

If you are a Business User who has chosen a name that includes Personal Data (for example, a sole proprietorship or family name in a company name), we will use and share such information for the provision of our Services in the same way we do with any company name. This may include, for example, displaying it on receipts and other transaction-identifying descriptions.

Fraud detection and loss prevention. We use Representatives' Personal Data to identify and manage risks that our Business Services might be used for fraudulent activities causing losses to Stripe, End Users, End Customers, Business Users, Financial Partners, and others. We also use information about you obtained from publicly available sources, third parties like credit bureaus and from our Services to address such risks, including to identify patterns of misuse and monitor for terms of service violations. Stripe may share Representatives' Personal Data with Business Users, our Financial Partners, and third party service providers, including phone verification providers, [Learn More](#), to verify the information provided by you and identify risk indicators. [Learn More](#). We also use and share Representatives' Personal Data to conduct due diligence, including conducting anti-money laundering and sanctions screening in accordance with applicable law.

Advertising. Where permitted by applicable law, and where required with your consent, we use and share Representatives' Personal Data with third parties, including Partners, so we can advertise and market our Services and Partner integrations. Subject to applicable law, including any consent requirements, we may advertise through interest-based advertising and track the efficacy of such ads. See our [Cookie Policy](#). We do not transfer your Personal Data to third parties in exchange for payment. However, we may provide your data to third party partners, like advertising partners, analytics providers, and social networks, who assist us in advertising our Services. [Learn more](#). We may also use your Personal Data, including your Stripe account activity, to evaluate your eligibility for and offer you Business Services or promote existing Business Services. [Learn more](#).

More. For further information about additional ways by which we may use and share Representatives' Personal Data, please see the *[More ways we collect, use, and share Personal Data](#)* section below.

1.4 Visitors

We collect, use, and share the Personal Data of Visitors. More details about how we collect, use, and share Visitors' Personal Data, along with the legal bases we rely on for processing such Personal Data, can be found in our [Privacy Center](#).

a. Personal Data we collect about Visitors

When you browse our Sites, we receive your Personal Data, either provided directly by you or collected through our use of cookies and similar technologies. See our [Cookie Policy](#) for more information. If you opt to complete a form on the Site or third party websites where our advertisements are displayed (like LinkedIn or Facebook), we collect the information you included in

the form. This may include your contact information and other information pertaining to your questions about our Services. We may also associate a location with your visit. [Learn More](#).

More. Further details about other types of Personal Data that we may collect from Visitors, including your online activity, can be found in the *[More ways we collect, use, and share Personal Data](#)* section below.

b. How we use and share Personal Data of Visitors

Personalization. We use the data we collect about you using cookies and similar technologies to measure engagement with the content on the Sites, improve relevancy and navigation, customize your experience (such as language preference and region-specific content), and curate content about Stripe and our Services that's tailored to you. For instance, as not all of our Services are available globally, we may customize our responses based on your region.

Advertising. Where permitted by applicable law, and where required with your consent, we use and share Visitors' Personal Data with third parties, including **Partners**, so we can advertise and market our Services and Partner integrations. Subject to applicable law, including any consent requirements, we may advertise through interest-based advertising and track the efficacy of such ads. See our [Cookie Policy](#). We do not transfer your Personal Data to third parties in exchange for payment, but we may provide your data to third party partners, like advertising partners, analytics providers, and social networks, who assist us in advertising our Services. [Learn more](#).

Engagement. As you interact with our Sites, we use the information we collect about and through your devices to provide opportunities for further interactions, such as discussions about Services or interactions with chatbots, to address your questions.

More. For more information about additional ways we may use and share Visitors' Personal Data, please see the *[More ways we collect, use, and share Personal Data](#)* section below.

2. More ways we collect, use, and share Personal Data

In addition to the ways described above, we also process your Personal Data as follows:

a. Collection of Personal Data

Online Activity. Depending on the Service used and how our Business Services are implemented by the Business Users, we may collect information related to:

The devices and browsers you use across our Sites and third party websites, apps, and other online services ("Third Party Sites").

Usage data associated with those devices and browsers and your engagement with our Services, including data elements like IP address, plug-ins, language preference, time spent on Sites and Third Party Sites, pages visited, links clicked, payment methods used, and the pages that led you to our Sites and Third Party Sites. We also collect activity indicators, such as mouse activity indicators, to help us detect fraud. [Learn More](#). See also our [Cookie Policy](#).

Communication and Engagement Information. We also collect information you choose to share with us through various channels, such as support tickets, emails, or social media. If you respond to emails or surveys from Stripe, we collect your email

address, name, and any other data you opt to include in your email or responses. If you engage with us over the phone, we collect your phone number and any other information you might provide during the call. Calls with Stripe or Stripe representatives may be recorded. [Learn More](#). Additionally, we collect your engagement data, like your registration for, attendance at, or viewing of Stripe events and any other interactions with Stripe personnel.

Forums and Discussion Groups. If our Sites allow posting of content, we collect Personal Data that you provide in connection with the post.

b. Use of Personal Data.

Besides the use of Personal Data described above, we use Personal Data in the ways listed below:

Analyzing, Improving, and Developing our Services. We collect and process Personal Data throughout our various Services, whether you are an End User, End Customer, Representative, or Visitor, to improve our Services, develop new Services, and support our efforts to make our Services more efficient, relevant, and useful to you. [Learn More](#). We may use Personal Data to generate aggregate and statistical information to understand and explain how our Services are used. Examples of how we use Personal Data to analyze, improve, and develop our products and services include:

Using analytics on our Sites, including as described in our Cookie Policy, to help us understand your use of our Sites and Services and diagnose technical issues.

Training machine learning models to power our Services and protect against fraud and other harm. [Learn more](#).

Analyzing and drawing inferences from Transaction Data to reduce costs, fraud, and disputes and increase authentication and authorization rates for Stripe and our Business Users.

Communications. We use the contact information we have about you to deliver our Services, [Learn More](#), which may involve sending codes via SMS for your authentication. [Learn More](#). If you are an End User, Representative, or Visitor, we may communicate with you using the contact information we have about you to provide information about our Services and our affiliates' services, invite you to participate in our events, surveys, or user research, or otherwise communicate with you for marketing purposes, in compliance with applicable law, including any consent or opt-out requirements. For example, when you provide your contact information to us or when we collect your business contact details through participation at trade shows or other events, we may use this data to follow up with you regarding an event, provide information requested about our Services, and include you in our marketing information campaigns. Where permitted under applicable law, we may record our calls with you to provide our Services, comply with our legal obligations, perform research and quality assurance, and for training purposes.

Social Media and Promotions. If you opt to submit Personal Data to engage in an offer, program, or promotion, we use the Personal Data you provide to manage the offer, program, or promotion. We also use the Personal Data you provide, along with the Personal Data you make available on social media platforms, for marketing purposes, unless we are not permitted to do so.

Fraud Prevention and Security. We collect and use Personal Data to help us identify and manage activities that could be fraudulent or harmful across our Services, enable our fraud detection Business Services, and secure our Services and transactions against unauthorized access, use, alteration or misappropriation of Personal Data, information, and funds. As part of the fraud prevention, detection, security monitoring, and compliance efforts for Stripe and its Business Users, we collect information from publicly available sources, third parties (such as credit bureaus), and via the Services we offer. In some instances, we may also collect information about you directly from you, or from our Business Users, Financial Partners, and other third parties for the same purposes. Furthermore, to protect our Services, we may receive details such as IP addresses and other identifying data about potential security threats from third parties. [Learn More](#). Such information helps us verify identities, conduct credit checks where lawfully permitted, and prevent fraud. Additionally, we might use technology to evaluate the potential risk of fraud associated with individuals seeking to procure our Business Services or arising from attempted transactions by an End Customer or End User with our Business Users or Financial Partners.

Compliance with Legal Obligations. We use Personal Data to meet our contractual and legal obligations related to anti-money laundering, Know-Your-Customer ("KYC") laws, anti-terrorism activities, safeguarding vulnerable customers, export control, and prohibition of doing business with restricted persons or in certain business fields, among other legal obligations. For example, we may monitor transaction patterns and other online signals and use those insights to identify fraud, money laundering, and other harmful activity that could affect Stripe, our Financial Partners, End Users, Business Users and others. [Learn More](#). Safety, security, and compliance for our Services are key priorities for us, and collecting and using Personal Data is crucial to this effort.

Minors. Our Services are not directed to children under the age of 13, and we request that they do not provide Personal Data to seek Services directly from Stripe. In certain jurisdictions, we may impose higher age limits as required by applicable law.

c. Sharing of Personal Data.

Besides the sharing of Personal Data described above, we share Personal Data in the ways listed below:

Stripe Affiliates. We share Personal Data with other Stripe-affiliated entities for purposes identified in this Policy.

Service Providers or Processors. In order to provide, communicate, market, analyze, and advertise our Services, we depend on service providers. These providers offer critical services such as providing cloud infrastructure, conducting analytics for the assessment of the speed, accuracy, and/or security of our Services, verifying identities, identifying potentially harmful activity, and providing customer service and audit functions. We authorize these service providers to use or disclose the Personal Data we make available to them to perform services on our behalf and to comply with relevant legal obligations. We require these service providers to contractually commit to security and confidentiality obligations for the Personal Data they process on our behalf. The majority of our service providers are based in the European Union, the United States of America, and India. [Learn More](#).

Financial Partners. We share Personal Data with certain Financial Partners to provide Services to Business Users and offer certain Services in conjunction with these Financial Partners. For instance, we may share certain Personal Data, such as payment processing volume, loan repayment data, and Representative contact information, with institutional investors and lenders who purchase loan receivables or provide financing related to Stripe Capital. [Learn More](#).

Others with Consent. In some situations, we may not offer a service, but instead refer you to others (like professional service firms that we partner with to deliver the Atlas Service). In these instances, we will disclose the identity of the third party and the information to be shared with them, and seek your consent to share the information.

Corporate Transactions. If we enter or intend to enter a transaction that modifies the structure of our business, such as a reorganization, merger, sale, joint venture, assignment, transfer, change of control, or other disposition of all or part of our business, assets, or stock, we may share Personal Data with third parties in connection with such transaction. Any other entity that buys us or part of our business will have the right to continue to use your Personal Data, subject to the terms of this Policy.

Compliance and Harm Prevention. We share Personal Data when we believe it is necessary to comply with applicable law; to abide by rules imposed by Financial Partners in connection with the use of their payment method; to enforce our contractual rights; to secure and protect the Services, rights, privacy, safety, and property of Stripe, you, and others, including against malicious or fraudulent activity; and to respond to valid legal requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, which may include authorities outside your country of residence.

3. Legal bases for processing Personal Data

For purposes of the General Data Protection Regulation (GDPR) and other applicable data protection laws, we rely on a number of legal bases to process your Personal Data. [Learn More](#). For some jurisdictions, there may be additional legal bases, which are outlined in the [Jurisdiction-Specific Provisions](#) section below.

a. Contractual and Pre-Contractual Business Relationships. We process Personal Data to enter into business relationships with prospective Business Users and End Users and fulfill our respective contractual obligations with them. These processing activities include:

- Creation and management of Stripe accounts and Stripe account credentials, including the assessment of applications to initiate or expand the use of our Services;

- Creation and management of Stripe Checkout accounts;

- Accounting, auditing, and billing activities; and

- Processing of payments and related activities, which include fraud detection, loss prevention, transaction optimization, communications about such payments, and related customer service activities.

b. Legal Compliance. We process Personal Data to verify the identities of individuals and entities to comply with obligations related to fraud monitoring, prevention, and detection, laws associated with identifying and reporting illicit and illegal activities, such as those under the Anti-Money Laundering ("AML") and Know-Your-Customer ("KYC") regulations, and financial reporting obligations. For example, we may be required to record and verify a Business User's identity to comply with regulations designed to prevent money laundering, fraud, and financial crimes. These legal obligations may require us to report our compliance to third parties and subject ourselves to third party verification audits.

c. Legitimate Interests. Where permitted under applicable law, we rely on our legitimate business interests to process your Personal Data. The following list provides an example of the business purposes for which we have a legitimate interest in processing your data:

- Detection, monitoring, and prevention of fraud and unauthorized payment transactions;

- Mitigation of financial loss, claims, liabilities or other harm to End Customers, End Users, Business Users, Financial Partners, and Stripe;

- Determination of eligibility for and offering new Stripe Services ([Learn More](#));

- Response to inquiries, delivery of Service notices, and provision of customer support;

- Promotion, analysis, modification, and improvement of our Services, systems, and tools, as well as the development of new products and services, including enhancing the reliability of the Services;

- Management, operation, and improvement of the performance of our Sites and Services, through understanding their effectiveness and optimizing our digital assets;

- Analysis and advertisement of our Services, and related improvements;

- Aggregate analysis and development of business intelligence that enable us to operate, protect, make informed decisions about, and report on the performance of our business;

- Sharing of Personal Data with third party service providers that offer services on our behalf and business partners that help us in operating and improving our business ([Learn More](#));

Enabling network and information security throughout Stripe and our Services; and

Sharing of Personal Data among our affiliates.

d. Consent. We may rely on consent or explicit consent to collect and process Personal Data regarding our interactions with you and the provision of our Services such as Link, Financial Connections, Atlas, and Identity. When we process your Personal Data based on your consent, you have the right to withdraw your consent at any time, and such a withdrawal will not impact the legality of processing performed based on the consent prior to its withdrawal.

e. Substantial Public Interest. We may process special categories of Personal Data, as defined by the GDPR, when such processing is necessary for reasons of substantial public interest and consistent with applicable law, such as when we conduct politically-exposed person checks. We may also process Personal Data related to criminal convictions and offenses when such processing is authorized by applicable law, such as when we conduct sanctions screening to comply with AML and KYC obligations.

f. Other valid legal bases. We may process Personal Data further to other valid legal bases as recognized under applicable law in specific jurisdictions. See the Jurisdiction-specific provisions section below for more information.

4. Your rights and choices

Depending on your location and subject to applicable law, you may have choices regarding our collection, use, and disclosure of your Personal Data:

a. Opting out of receiving electronic communications from us

If you wish to stop receiving marketing-related emails from us, you can opt-out by clicking the unsubscribe link included in such emails or as described [here](#). We'll try to process your request(s) as quickly as reasonably practicable. However, it's important to note that even if you opt out of receiving marketing-related emails from us, we retain the right to communicate with you about the Services you receive (like support and important legal notices) and our Business Users might still send you messages or instruct us to send you messages on their behalf.

b. Your data protection rights

Depending on your location and subject to applicable law, you may have the following rights regarding the Personal Data we process about you as a data controller:

The right to request confirmation of whether Stripe is processing Personal Data associated with you, the categories of personal data it has processed, and the third parties or categories of third parties with which your Personal Data is shared;

The right to request access to the Personal Data Stripe processes about you ([Learn More](#));

The right to request that Stripe rectify or update your Personal Data if it's inaccurate, incomplete, or outdated;

The right to request that Stripe erase your Personal Data in certain circumstances as provided by law ([Learn More](#));

The right to request that Stripe restrict the use of your Personal Data in certain circumstances, such as while Stripe is considering another request you've submitted (for instance, a request that Stripe update your Personal Data);

The right to request that we export the Personal Data we hold about you to another company, provided it's technically feasible;

The right to withdraw your consent if your Personal Data is being processed based on your previous consent;

The right to object to the processing of your Personal Data if we are processing your data based on our legitimate interests; unless there are compelling legitimate grounds or the processing is necessary for legal reasons, we will cease processing your Personal Data upon receiving your objection ([Learn More](#));

The right not to be discriminated against for exercising these rights; and

The right to appeal any decision by Stripe relating to your rights by contacting Stripe's Data Protection Officer ("DPO") at dpo@stripe.com, and/or relevant regulatory agencies.

You may have additional rights, depending on applicable law, over your Personal Data. For example, see the Jurisdiction-specific provisions section under United States below.

c. Process for exercising your data protection rights

To exercise your data protection rights related to Personal Data we process as a data controller, visit our [Privacy Center](#) or contact us as outlined below. For Personal Data we process as a data processor, please reach out to the relevant data controller (Business User) to exercise your rights. If you contact us regarding your Personal Data we process as a data processor, we will refer you to the relevant data controller to the extent we are able to identify them.

5. Security and Retention

We make reasonable efforts to provide a level of security appropriate to the risk associated with the processing of your Personal Data. We maintain organizational, technical, and administrative measures designed to protect the Personal Data covered by this Policy from unauthorized access, destruction, loss, alteration, or misuse. [Learn More](#). Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure.

We encourage you to assist us in protecting your Personal Data. If you hold a Stripe account, you can do so by using a strong password, safeguarding your password against unauthorized use, and avoiding using identical login credentials you use for other services or accounts for your Stripe account. If you suspect that your interaction with us is no longer secure (for instance, you believe that your Stripe account's security has been compromised), please **contact us** immediately.

We retain your Personal Data for as long as we continue to provide the Services to you or our Business Users, or for a period in which we reasonably foresee continuing to provide the Services. Even after we stop providing Services directly to you or to a Business User that you're doing business with, and even after you close your Stripe account or complete a transaction with a Business User, we may continue to retain your Personal Data to:

Comply with our legal and regulatory obligations;

Enable fraud monitoring, detection, and prevention activities; and

Comply with our tax, accounting, and financial reporting obligations, including when such retention is required by our contractual agreements with our Financial Partners (and where data retention is mandated by the payment methods you've used).

In cases where we keep your Personal Data, we do so in accordance with any limitation periods and record retention obligations imposed by applicable law. [Learn More](#).

6. International Data Transfers

As a global business, it's sometimes necessary for us to transfer your Personal Data to countries other than your own, including the United States. These countries might have data protection regulations that are different from those in your country. When transferring data across borders, we take measures to comply with applicable data protection laws related to such transfer. In certain situations, we may be required to disclose Personal Data in response to lawful requests from officials, such as law enforcement or security authorities. [Learn More](#).

If you are located in the European Economic Area ("EEA"), the United Kingdom ("UK"), or Switzerland, please refer to our [Privacy Center](#) for additional details. When a data transfer mechanism is mandated by applicable law, we employ one or more of the following:

Transfers to certain countries or recipients that are recognized as having an adequate level of protection for Personal Data under applicable law.

EU Standard Contractual Clauses approved by the European Commission and the UK International Data Transfer Addendum issued by the Information Commissioner's Office. You can obtain a copy of the relevant Standard Contractual Clauses. [Learn More](#).

Other lawful methods available to us under applicable law.

Stripe, Inc. complies with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce and as applicable. [Learn More](#).

Stripe's privacy practices, as described in this Privacy Policy, comply with the Cross Border Privacy Rules System ("CBPR") and Privacy Rules for Processor ("PRP") systems. These systems provide a framework for organizations to ensure protection of personal data transferred among participating economies. Where CBPR and/or PRP are recognized as a valid transfer mechanism under applicable law, Stripe will transfer Personal Data in accordance with the CBPR and PRP certifications Stripe has obtained. More information about the framework can be found [here](#) and [here](#). If you have unresolved privacy or data use concerns that we have not addressed satisfactorily, please contact our U.S. based third-party dispute resolution provider (free of charge) at <https://feedback-form.truste.com/watchdog/request>. To view the status of our certifications, please click [here](#) (CBPR) and [here](#) (PRP).

7. Updates and notifications

We may change this Policy from time to time to reflect new services, changes in our privacy practices or relevant laws. The "Last updated" legend at the top of this Policy indicates when this Policy was last materially revised. Any changes are effective the latter of when we post the revised Policy on the Services or otherwise provide notice of the update as required by law.

We may provide you with disclosures and alerts regarding the Policy or Personal Data collected by posting them on our website and, if you are an End User or Representative, by contacting you through your Stripe Dashboard, email address and/or the physical address listed in your Stripe account.

8. Jurisdiction-specific provisions

Australia. “Personal Data” includes “personal information” as defined under applicable privacy laws in Australia, including the Privacy Act 1988 (Cth) as amended from time to time.

If we use personal information to make automated decisions that could reasonably be expected to significantly affect your rights or interests, we will provide the legally required information and transparency via our [Privacy Center](#), and/or on a case by case basis.

If you are an Australian resident and dissatisfied with our handling of any complaint you raise under this Policy, you may consider contacting the Office of the Australian Information Commissioner.

Brazil. You may exercise your rights by contacting our DPO Adi Gilad at dpo@stripe.com. Brazilian residents, for whom the Lei Geral de Proteção de Dados Pessoais (“LGPD”) applies, have rights set forth in Article 18 of the LGPD.

Canada. As used in this Policy, “applicable law” includes the Federal Personal Information Protection and Electronic Documents Act (“PIPEDA”), the Personal Information Protection Act, SBC 2003 c 63, in British Columbia, the Personal Information Protection Act, SA 2003 c P-6.5, in Alberta, and the Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39-1 (“Quebec Private Sector Act”), in Quebec. [Learn more](#). “Personal Data” includes “personal information” as defined under those laws.

Stripe's Chief Privacy Officer is the person in charge of personal information, including under the Quebec Private Sector Act. You may contact them via email at privacy@stripe.com. When Stripe collects Personal Data belonging to Canadian (including Quebec) residents, it transfers that data to data centers in the United States. When Stripe relies on service providers to process Personal Data as described herein, those service providers may also be located outside of Canada or Quebec.

You have the right to request access or rectification of the Personal Data Stripe holds related to you or to withdraw any consent given to the processing of such personal data. You may exercise those rights by contacting Stripe's Chief Privacy Officer at privacy@stripe.com. If you are an End Customer, you should contact the Business User with which you transacted to exercise your rights.

EEA and UK. You may exercise your rights by contacting our DPO at dpo@stripe.com. If you are a resident of the EEA or the Stripe entity accountable for your Personal data is otherwise subject to the GDPR, and you believe our processing of your information contradicts the GDPR, you may direct your questions or complaints to the Irish Data Protection Commission. If you are a resident of the UK, direct your questions or concerns to the UK Information Commissioner's Office. You also have additional rights under the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. [Learn More](#).

India. In this Policy, “applicable law” includes the Digital Personal Data Protection Act (“DPDPA”) once the DPDPA enters into effect. Further, the term “data controller” includes “data fiduciaries,” and the term “data subject” includes “data principal,” both as defined in the DPDPA.

In some cases, and as permitted under the DPDPA, we may rely on “legitimate use” as a legal basis. For example, we might do so when you voluntarily provide your Personal Data to us. Where we are required to obtain your explicit and informed consent, we will do so on a case by case basis. “Consent Managers” as defined under the DPDPA may submit a request to revoke or provide consent using the methods described in the Contact Us section below, or as set out in the following paragraph, or via other means made available by Stripe in the future. We may ask for proof of authorization and identity before processing such a request.

You have the right to contact Stripe to nominate another individual, who may, in the event of your death or incapacity, exercise your rights under this Privacy Policy and under the DPDPA and implementing regulations.

In certain cases, you may be asked to consent to the collection and processing of your Aadhaar number by Stripe India Private Limited and/or its third party verification partner(s). The purpose of this collection is to facilitate the identification verification process as required under applicable laws. Your provision of Aadhaar details is purely voluntary, and you may provide other identification documents as may be accepted by us from time to time. You will not be denied service merely for not submitting Aadhaar details.

If you have any questions or complaints regarding the processing of your Personal Data in India, or if you want to receive this Policy or communicate with us about privacy in one of India's official languages, please **contact our Nodal and Grievance Officer. [Learn More](#)**. Alternatively, you may contact our DPO at dpo@stripe.com. If we are unable to address your complaint or grievance, you have the right to escalate the matter to the Data Protection Board of India.

Indonesia. In this Policy, "applicable law" includes Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, and Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems, and from September 2024, Law No. 27 of 2022 concerning Personal Data Protection ("PDP Law"). If you have any questions or complaints about this Policy, please contact our DPO at dpo@stripe.com.

Japan. In this Policy, "applicable law" includes the Act on the Protection of Personal Information ("APPI"). When we transfer Personal Data of data subjects in Japan to jurisdictions not recognized as 'adequate' by the Personal Information Protection Commission, we enter into written agreements with any third parties located outside of Japan. These written agreements provide rights and obligations equivalent to those provided under the Japanese Act on the Protection of Personal Information. For more information on how we ensure that third parties protect your data and where your data is located, please see above or contact us as described below. For a description of foreign systems and frameworks that may affect the implementation of equivalent measures by the third party, see [here](#). In some cases, and as permitted under the APPI, we may rely on "public interest" as a legal basis, such as fraud detection and loss prevention.

Malaysia. If you have any questions or complaints about this Policy, please contact our DPO at dpo@stripe.com.

Singapore. In this Policy, "applicable law" includes the Personal Data Protection Act 2012 ("PDPA") (No. 26 of 2012) as amended from time to time. In some cases, and as permitted under the PDPA, we may rely on "deemed consent" as a legal basis. For example, we do so when you voluntarily provide your personal data to us. If you have any questions or complaints about this Policy, please contact our DPO at dpo@stripe.com.

Switzerland. In this Policy, "applicable law" includes the Swiss Federal Act on Data Protection ("FADP"), as revised. To exercise your rights under the FADP, please contact our DPO at dpo@stripe.com. You may also have additional rights under the Swiss-U.S. Data Privacy Framework. **[Learn More](#)**.

Thailand. In this Policy, "applicable law" includes the Personal Data Protection Act 2019 ("PDPA"). If we rely on certain legal bases (such as "legal obligation" or "contractual necessity" and you do not provide us with your Personal Data, we may not be able to lawfully provide you services. If you have any questions or complaints about this Policy, please contact our DPO at dpo@stripe.com. Where required, we have put in place appropriate safeguards for the cross-border transfer of Personal Data from Thailand, including the EU Standard Contractual Clauses as adapted for Thailand data transfers in accordance with the Notification of the Personal Data Protection Committee on Criteria for the Protection of Personal Data Sent or Transferred to a Foreign Country Pursuant to Section 29 of the Personal Data Protection Act, B.E. 2562 B.E. 2566 (2023).

United States. If you are a consumer located in the United States ("US"), we process your personal information in accordance with US federal and state privacy laws. For additional details, please review the information below and see our additional U.S. Privacy Disclosures [here](#). Stripe uses cookies, including advertising cookies, as described in our [Cookie Policy](#).

Your Rights and Choices. As a US consumer and subject to certain limitations under US privacy laws, you may have choices regarding our use and disclosure of your Personal Data. In addition to the [above rights](#), you may also have the rights listed in this section. Please see our Privacy Center to [learn more](#) about data subject rights metrics and [learn more](#) about the laws under which these rights may apply.

Exercising the right to know: You have a right to request additional information about the categories of personal information collected, sold, disclosed, or shared; purposes for which this personal information was collected, sold, or

shared; categories of sources of personal information; and categories of third parties with whom we disclosed or shared this personal information.

Exercising the right to opt-out from a sale or sharing: We do not transfer your personal data to third parties in exchange for payment. However, as noted above, we may provide the data to third party partners, such as advertising partners, analytics providers, and social networks, who assist us in advertising our products and Services to you. Because these third parties may use the data Stripe provides for their own purposes, Stripe's provision of data to these parties may be considered a data "sale" or "sharing" (for behavioral advertising) as those terms are defined under the CCPA and other applicable US privacy laws. You can opt out of targeted advertising and any related data "sales" or "sharing" (for behavioral advertising) [here](#).

Exercising the right to limit the use or sharing of Sensitive Personal Information: We do not sell or share (for behavioral advertising) Sensitive Personal Information as defined by US privacy laws and have not done so in the past 12 months. Learn more about our collection and use of Sensitive Personal Information over the last 12 months [here](#).

Profiling with legal or similarly significant effects: In the event that we engage in profiling or automated decision making for which applicable law entitles you to an opt out we will provide you with notice of how to exercise that opt-out right.

Appeal: If you wish to appeal any of our decisions regarding a rights request under US privacy laws, you may do so by contacting Stripe's Data Protection Officer ("DPO") at dpo@stripe.com.

To submit a request to exercise any of the rights described above, please contact us using the methods described in the Contact Us section below. Please note that rights under some U.S. state laws do not apply to Personal Data we collect, process, and disclose when you act as a consumer to obtain financial products or services from Stripe for personal, family, or household purposes. The federal Gramm-Leach Bliley Act may govern how Stripe shares and protects that data instead. See our **US Consumer Privacy Notice** below for more information.

We will verify your request by asking you to send it from the email address associated with your account or requiring you to provide information necessary to verify your identity, including name, address, transaction history, photo identification, and other information associated with your account.

You may designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise your rights under the CCPA and other applicable US privacy laws. Your agent may submit a request on your behalf by contacting us using the methods described in the Contact Us section below. We may still require you to directly verify your identity and confirm that you gave the authorized agent permission to submit the request.

Global Privacy Control signals. Stripe honors the Global Privacy Control (GPC) opt-out preference signals. [Learn More](#).

9. Contact us

If you have any questions or complaints about this Policy, please **contact us**. If you are an End Customer (i.e., an individual doing business or transacting with a Business User), please refer to the privacy policy or notice of the Business User for information regarding the Business User's privacy practices, choices and controls, or contact the Business User directly.

10. US Consumer Privacy Notice

The following Consumer Privacy Notice applies to you if you are an individual who resides in the United States and obtains financial services from Stripe primarily for your own personal, family, or household purposes.

Last updated: January 16, 2025

FACTS WHAT DOES STRIPE DO WITH YOUR PERSONAL INFORMATION?

Why? Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- What?**
- Social Security Number
 - Contact details
 - Account balances and transaction history
 - Payment, transaction, and purchase information and history

When you are *no longer* our customer, we continue to share your information as described in this notice.

How? All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Stripe chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Stripe Share?	Can you limit this sharing
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes - to offer our products and Services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes - information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes - information about your creditworthiness	No	We don't share
For our affiliates to market to you	No	We don't share
For nonaffiliates to market to you (for data not collected through Financial Connections)	Yes	Yes
For nonaffiliates to market to you (for data collected through Financial Connections)	No	We don't share

Login to your Link account at app.link.com/settings and toggle off data sharing from the Messaging menu.

To limit our sharing

Please note: If you are a new customer, we can begin sharing your information 30 days from the date we sent this notice. When you are no longer our customer, we continue to share your information as described in this notice.

However, you can contact us at any time to limit our sharing.

Questions?

Contact us at privacy@stripe.com or visit us at <https://support.link.com>

Who we are

Who is providing this notice?

Stripe, Inc., Stripe Payments Company, and their affiliates that provide consumers services in the U.S.

What we do

How does Stripe protect my personal information?

To protect your personal information from unauthorized access, destruction, loss, alteration, or misuse we use security measures to comply with federal law. These measures include computer safeguards and secured files and buildings. We impose access controls along with ongoing monitoring to prevent data misuse, and we require our service providers to take similar steps to protect your information.

How does Stripe collect my personal information?

We collect your personal information, for example, when you

- open a Link account;
- ask Stripe to process a payment for goods or services;
- provide bank account information to Stripe using Financial Connections

We also collect your personal information from others, such as affiliates or other companies.

Why can't I limit all sharing?

Federal law gives you the right to limit only

- sharing for affiliates' everyday business purposes — information about your creditworthiness
- affiliates from using your information to market to you
- sharing for nonaffiliates to market to you.

State laws and individual companies may give you additional rights to limit sharing. See the Other Important Information section below for more information on your rights under state law.

What happens when I limit sharing for an account I hold jointly with someone else?

Your choices will apply to everyone on your account.

Definitions

Affiliates	<p>Companies related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none">• <i>Our affiliates include companies operating under the Stripe name, such as Stripe Technology Europe, Ltd. and Stripe Payments UK, Ltd.</i>
Nonaffiliates	<p>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none">• <i>Nonaffiliates with which we share personal information include service providers that perform services or functions on our behalf, Business Users with which you choose to transact, partners with which we share data to provide you with services, and advertising partners, analytics providers, and social networks, who assist us in advertising our Services to you.</i>
Joint Marketing	<p>A formal agreement between non-affiliated financial companies that together market financial products or services to you.</p> <ul style="list-style-type: none">• <i>Our joint marketing partners include financial companies we partner with to provide you with financial services.</i>

Other important information

Vermont: If your account with us is associated with a Vermont billing address, we will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures. For joint marketing, we will only disclose your name, contact information, and information about your transactions. Additional information concerning our privacy policies can be found in our [Privacy Policy](#) and [Privacy Center](#).

California: If your account with us is associated with a California billing address, we will not disclose Personal Data we collect about you except to the extent permitted under California law. For instance, we may disclose your Personal Data as necessary to process transactions or provide products and services you request, at your instruction, as required for institution risk control, and to safeguard against fraud, identity theft, and unauthorized transactions.

For additional information about our privacy practices, please visit the [Stripe Privacy Center](#).

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

Acquirer Disclosure

Cross River Bank

Deutsche Bank

Goldman Sachs Bank USA

PNC Bank

Issuing Bank Terms

Payment Method Terms

User Bank Debit Authorizations

Prohibited & Restricted Businesses