Permitting authorities use SolarAPP+'s standardized plan review software to work

Registration

CREATE ACCOUNT

Account-Type

As citie ewable

* First Name

* Last Name

* Email

* Password

* Confirm Password

Password must contain:

- Contain eight (8) or more characters.
- Contain one (1) or more upper- and lower-case character
- Contain one (1) or more numbers.
- Contain one (1) or more of the following special characters:
  ~!@#$%\^&*()_+\-={}|[\]\?,.\/;:"'
- **Not** contain user email or name

☐ By checking this box, you are certifying that you have read, and agree to our Terms of Use and Privacy Policy.

☐ Please send me SolarAPP+ announcements and updates.

CREATE ACCOUNT

SolarAPP+ Privacy Policy

Effective August 31, 2021.

This Privacy Policy explains how Alliance for Sustainable Energy, LLC (“Alliance”, “we”, or “us”) collects, uses, and shares information about you when you use the permitting review tool available on solarapp.nrel.gov webpage (“Web Tool”) which is provided by Alliance as Management and Operating Contractor of the National Renewable Energy Laboratory (“NREL”) under Prime Contract No. DE-AC36-08GO28308 for the United States Department of Energy (“DOE”), or when you otherwise interact with us or receive a communication from us about the Web Tool.

If you do not agree with our policies and practices, your choice is not to use the Web Tool. By using the Web Tool, you consent to the privacy practices described in this Privacy Policy. By providing any information discussed herein, you are representing and warranting to Alliance that you are authorized to disclose such information for the purposes set forth in this Privacy Policy.

This Web Tool is intended for use by 1) authorities having jurisdiction (“AHJs”) which are authorized permitting agencies, and 2) applicants (“Applicants”) for permits. Unless otherwise indicated, this Privacy Policy shall apply to both AHJs and Applicants. By submitting any information to Alliance via or in association with this Web Tool, you are representing and warranting to Alliance that you have the authority to disclose that information.

Unless otherwise stated herein, and/or unless you choose to provide such information to us, we collect no personal information about you or other information from you when you visit or use this Web Tool. Furthermore, unless otherwise stated herein, we will not sell or otherwise share any personal information about you, or other information received from you with any third parties.

Types of Information Collected and How It is Handled

1. We collect and store certain information automatically. This information includes:

   The Internet Protocol (IP) address of the domain from which you access the internet (i.e. 123.456.789.012) whether yours individually or provided as a proxy by your Internet Service Provider (ISP); the date and time you access the Web Tool; the pages you peruse (recorded by the text and graphics files that compose that page) and, the internet address of the Web Tool from which you linked directly to our Web Tool.

   We may use the summary statistics to help us make this Web Tool more useful to visitors, such as assessing what information is of most and least interest to visitors, and for other purposes such as determining the Web Tool’s technical design specifications and identifying system performance or problem areas. This information is shared with the support staff of this Web Tool and is used only as a source of anonymous statistical information.

2. To create an account, you must provide your first and last name, a username and password for your account, your email address, the business license number(s) for your organization, and the name and business address of your organization.

   We use this information to maintain the security of the Web Tool, to ensure you are authorized to access and use restricted portions of this Web Tool, and to manage your account and our relationship with you. We also provide some or all of this information to third parties with legitimate business interests, including to the governmental jurisdiction in which you apply, via this Web Tool, for a permit to construct, install, and/or operate a residentia panel system (a “PV Permit”)). The governmental jurisdiction may or may not make this information available t public to comply with its open records policies. By providing your email address, you are consenting to receive updates about SolarAPP+ via email. You may opt out (i.e., unsubscribe) from these emails at anytime by contact **solarapp@nrel.gov.**

3. To apply for a PV Permit using the Web Tool, you must provide information about the project for which you are applying, including an address at which the project will take place, a jurisdiction in which the project exists, and technical specifications regarding the project (e.g., generation capacity, structural details, components or systems included, etc.).

   We provide this information to the relevant governmental jurisdiction to assist in their determination of whether or not to issue the requested PV Permit. We also provide some or all of this information to other third parties with legitimate business interests. The governmental jurisdiction, the U.S. Government, and/or the DOE may or may not make this information available to the public to comply with open records laws and/or policies.

4. You may choose to provide us with other information, such as in an e-mail message containing your ideas, suggestions, comments, or questions (“Feedback”).

   We may use your Feedback to improve, revise, or update the Web Tool, or to respond to your request. There are times when your message is forwarded, as e-mail, to other Alliance employees who may be better able to help you or who are responsible for maintaining the Web Tool.

   Any Feedback about this Web Tool that you provide to Alliance is entirely voluntary, and by providing Feedback you are agreeing that Alliance may use such Feedback without restriction and without compensation or obligation to you. To the extent any license would be required to utilize or implement your Feedback, you automatically grant Alliance, when submitting such Feedback, a worldwide, royalty-free, perpetual, irrevocable, non-exclusive, transferable, and sublicensable license under any rights necessary for such use or implementation.

Situations When Disclosure of Data May Occur

Notwithstanding anything to the contrary herein, we reserve the right to disclose your information that we believe, in good faith, is appropriate or necessary to (i) take precautions against liability, (ii) protect ourselves and others from fraudulent, abusive, or unlawful uses or activity, (iii) investigate and defend ourselves against any third-party claims or allegations, (iv) protect the security or integrity of the Web Tool and any facilities or equipment used to make the Web Tool available, (v) protect our property or other legal rights (including, but not limited to, enforcement of our agreements), or the rights, property, or safety of others, (vi) comply with the audit, inspection, and copying requirements of our Prime Contract with the United States Government, or (vii) to comply with relevant open records laws.

We also may disclose your information as may be described in a notice to you at the time the information is collected, or in any other manner to which you consent. We will attempt to inform you of how we are going to use your information. We will achieve this through this Privacy Policy and by informing you how your information is used each time we collect it.

Changing Data Provided

You may, of course, decline to share certain information with us, in which case we may not be able to provide all features and functionality of the Web Tool to you. You may update, correct, or delete your account at any time. If you wish to access or amend any other information we hold about you, or request that we delete any information about you that we have obtained through the Web Tool, you may submit your request by contacting at us at solarapp@nrel.gov. Requests are subject to verification of identity. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

Timeline of Storing of Data

We will attempt to keep your data for no longer than necessary. The length of time we retain it will depend on any legal obligations we have (such as governmental reporting purposes), the nature of any contracts we have in place with you, the existence of your consent and/or our legitimate business interests.

Privacy Policy Subject to Change

Alliance may make changes to this Privacy Policy from time to time. If we make changes, we will post the amended Privacy Policy to this Web Tool and update the Effective Date above. By continuing to access or use the Web Tool on or after the Effective Date of the revised Privacy Policy, you agree to be bound by the revised Privacy Policy. If you do not agree to the revised Privacy Policy, you must stop accessing and using the Web Tool before the changes become effective. You are responsible for checking the Privacy Policy for changes and your continued use of the Web Tool constitutes acceptance of updated Privacy Policy.

General

Capitalized terms used but not defined in this Privacy Policy have the meanings given to them in the Terms of Use.

Terms of Service for Using the SolarAPP+

Effective August 31, 2021

INTRODUCTION

These Terms of Use (“Terms”) are between you and Alliance for Sustainable Energy, LLC (“Alliance”, “we”, or “us”) and govern your access to and use of the permitting review tool available on solarapp.nrel.gov webpage (“Web Tool”), which is provided by Alliance as Management and Operating Contractor of the National Renewable Energy Laboratory (“NREL”) under Prime Contract No. DE-AC36-08GO28308 (“Prime Contract”) for of the United States Department of Energy (“DOE”). By accessing or using the Web Tool, you agree to be bound by these Terms. If you are accepting these Terms on behalf of another legal entity, including your employer, another business, a government, etc., you represent that you are an authorized representative of that entity with full legal authority to bind such entity to these terms. If you do not agree to these Terms, you must not use this Web Tool.

This Web Tool is intended for use by 1) authorities having jurisdiction (“AHJs”) which are authorized permitting agencies, and 2) applicants (“Applicants”) for permits. Unless otherwise indicated, these terms shall apply to both AHJs and Applicants. By submitting any information to Alliance via or in association with this Web Tool, you are representing and warranting to Alliance that you have the authority to disclose that information.

NOTICE

Alliance is not permitting agency or jurisdiction and has no authority to issue permits of any kind. For AHJ’s, Alliance is not liable for the issuance of permits which do not meet the AHJ’s typical requirements, or which fail to comply with AHJ’s permit standards. AHJ’s must review all submissions to determine if issuing a permit is appropriate. AHJ’s remain exclusively responsible for the review and approval of permit applications. It is not recommended to rely solely on the Web Tool for the approval or issuance of a permit.

For Applicants, Alliance is not liable for the failure of any permits to issue or the failure of any applications to be submitted. Applicants must contact the relevant jurisdiction to obtain any permit. Applicants remain exclusively responsible for the timely submission of any required information for any permit application directly to the relevant jurisdiction. It is not recommended to rely solely on the Web Tool for the submission or approval of Applicant’s permit application.

Alliance, its officers, employees, agents, or representatives shall not be liable for any damages of any kind arising from your use of the linked online payment service. Nothing contained in this Web Tool constitutes or is intended to constitute legal advice from Alliance or any of its agencies, officers, employees, agents, or representatives.

PRIVACY AND SECURITY

This Web Tool may collect personal information from users, both AHJs and Applicants. By using this Web Tool and/or agreeing to these Terms, you consent to the collection, storage, and processing of your personal information/data as set forth in the **Privacy Policy**.

This Web Tool may be monitored by the U.S. government and any agency thereof (“U.S. Government”), by Alliance, or by others on their behalf, to ensure it remains available to all users and for security purposes to protect information in the system. By using the Web Tool, you expressly consent to these monitoring activities.

Unauthorized attempts to defeat or circumvent security features, to use the system for other than intended purposes, to deny service to authorized users, to access, obtain, alter, damage, or destroy information, or otherwise interfere with t system or its operation are prohibited. Evidence of such acts may be disclosed to law enforcement authorities and re

in criminal prosecution under the Computer Fraud and Abuse Act of 1986 (Pub. L. 990474) and the National Information Infrastructure Protection Act of 1996 (Pub. L. 104-294), (18 U.S.C. 1030), or other applicable criminal laws.

SYSTEM REQUIREMENTS

You are solely responsible for ensuring that your systems meet the hardware, software and any other applicable system requirements for the Web Tool. Alliance will have no obligations or responsibility under this Agreement for issues caused by your use of any third-party hardware or software not provided by Alliance.

YOUR ACCOUNT AND ACCOUNT SECURITY

To use certain features of the Web Tool, you may be required to create an account and provide Alliance with a username, password, and certain other information about yourself, as set forth in the **Privacy Policy**. When registering, you must fill in all mandatory fields with accurate, current, and complete information about yourself as prompted in the registration form and keep this information up to date. Alliance has the right to suspend or terminate your account or refuse any and all use of the Web Tool if it suspects your account information is inaccurate, not current, or incomplete.

You are solely responsible for maintaining the confidentiality of the password and username you provided during the registration process, and you are fully responsible for all activities that occur under your password or account. You agree to promptly notify Alliance if you discover or suspect any unauthorized use of your account or any other breach of security. You may not license, sell, or transfer your account without prior written permission from Alliance.

OWNERSHIP AND FEEDBACK

The Web Tool is made available on a limited access basis, and no ownership right is conveyed to you, irrespective of any use of terms such as “license”, “purchase”, or “sale”. Alliance and any third parties, as applicable, have and retain all right, title and interest, including all intellectual property rights, in and to all protectable aspects of the Web Tool.

Any ideas, suggestions, and feedback about this Web Tool that you provide to Alliance are entirely voluntary, and by providing such ideas, suggestions, and feedback (“Feedback”) you are agreeing that Alliance may use such Feedback without restriction and without compensation or obligation to you. To the extent any license would be required to utilize or implement your Feedback, you automatically grant Alliance, when submitting such Feedback, a worldwide, royalty-free, perpetual, irrevocable, non-exclusive, transferable, and sublicensable license under any rights necessary for such use or implementation.

PUBLICATION AND NON-ENDORSEMENT

You must not to use the names or marks of the U.S. Government, the DOE, NREL, or Alliance to endorse or promote any product, service, or entity without specific prior written authorization from the U.S. Government, DOE, or Alliance, as appropriate. All trademarks and service marks contained in or displayed on this Web Tool are the intellectual property of their respective owners. Any commercial use of the materials stored on this Web Tool is strictly prohibited without the prior written approval of Alliance.

INDEMNIFICATION REQUIREMENTS

EXCEPT TO THE EXTENT PROHIBITED BY LAW, YOU AGREE TO INDEMNIFY THE U.S. GOVERNMENT, DOE, ALLIANCE, AND THEIR RESPECTIVE SUBSIDIARIES, AFFILIATES, OFFICERS, AGENTS, AND EMPLOYEES AGAINST ANY THIRD-PARTY CLAIM OR DEMAND, INCLUDING REASONABLE ATTORNEYS' FEES, ARISING OUT OF OR RELATED TO YOUR VIOLATION OF THESE TERMS, YOUR VIOLATION OF APPLICABLE LAWS OR REGULATIONS, OR YOUR USE OF THE WEB TOOL.

DISCLAIMER OF WARRANTIES

THIS WEB TOOL IS PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ALLIANCE AND THE UNITED STATES GOVERNMENT DO NOT WARRANT THAT THE WEB TOOL OR ANY DATA AVAILABLE VIA THE WEB TOOL IS ACCURATE, COMPLETE, RELIABLE, CURRENT, OR ERROR FREE. ALLIANCE DOES NOT CONTROL, ENDORSE, OR TAKE RESPONSIBILITY FOR ANY THIRD-PARTY DATA PROVIDED VIA THE WEB TOOL OR THE ACTIONS OF ANY THIRD PARTY OR USER. WHILE ALLIANCE ATTEMPTS TO MAKE YOUR ACCESS TO AND USE OF THE WEB TOOL SAFE, ALLIANCE DOES NOT REPRESENT OR WARRANT THAT THE WEB TOOL OR SERVERS ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. NEITHER ALLIANCE NOR ANY THIRD-PARTY PROVIDERS OF DATA AVAILABLE VIA THE WEB TOOL HAVE ANY OBLIGATION TO PROVIDE UPDATES, SUPPORT, CONSULTING, TRAINING, OR ASSISTANCE OF ANY KIND WHATSOEVER WITH REGARD TO ANY DATA AVAILABLE VIA THE WEB TOOL OR USE THEREOF.

LIMITATION OF LIABILITYIN NO EVENT SHALL ALLIANCE, THE U.S. GOVERNMENT, OR ANY THIRD PARTY PROVIDER OF DATA AVAILABLE VIA THE WEB TOOL, NOR ANY OF THEIR OFFICERS, AGENTS, OR EMPLOYEES, BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER, INCLUDING (BUT NOT LIMITED TO) ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING FROM OR RELATING TO THESE TERMS, THE WEB TOOL, OR ANY DATA AVAILABLE VIA THE WEB TOOL. ACCESS TO, AND USE OF, THE WEB TOOL IS AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR DEVICE OR COMPUTER SYSTEM, OR LOSS OF DATA RESULTING THEREFROM. IN NO EVENT WILL THE AGGREGATE LIABILITY OF THE ABOVE ENTITIES EXCEED TEN U.S. DOLLARS ($10). THE LIMITATIONS OF THIS SECTION WILL APPLY TO ANY THEORY OF LIABILITY, INCLUDING THOSE BASED ON WARRANTY, CONTRACT, STATUTE, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN IF THE ABOVE ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGE, AND EVEN IF ANY REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED ITS ESSENTIAL PURPOSE. THE FOREGOING LIMITATION OF LIABILITY WILL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW IN THE APPLICABLE JURISDICTION.

TERMS SUBJECT TO CHANGE

Alliance may make changes to these Terms from time to time. If we make changes, we will post the amended Terms to this Web Tool and update the Effective Date above. By continuing to access or use the Web Tool on or after the Effective Date of the revised Terms, you agree to be bound by the revised Terms. If you do not agree to the revised Terms, you must stop accessing and using the Web Tool before the changes become effective. You are responsible for checking the Terms for changes and your continued use of the Web Tool constitutes acceptance of updated Terms.

TERMINATION

Alliance has no obligation to continue to support, maintain, and/or operate the Web Tool and may cease to do so and/or terminate the Web Tool at any time with or without notice to AHJs and/or Applicants.

Alliance may immediately terminate your access to the Web Tool and, should you have an account on the Web Tool, your account, for any reason (or for no reason), without warning. You may terminate your account at any time, for any reason, by contacting solarapp@nrel.gov. Even after termination, these Terms, including (but not limited to) the PRIVACY AND SECURITY section, the OWNERSHIP AND FEEDBACK section, the INDEMNITY, DISCLAIMER, AND LIMITATION OF LIABIITY section, the GOVERNING LAW AND JURISDICTION section, and the GENERAL section, will remain in effect.

GOVERNING LAW AND JURISDICTION

Any claims arising out of or relating to these Terms or this Web Tool will be governed exclusively by the laws of the United States of America and the State of Colorado, without giving effect to their conflict of laws principles. You expressly consent to the exclusive forum, jurisdiction, and venue of the Courts of the State of Colorado and the United States District Court for the District of Colorado in any and all actions, disputes, or controversies relating to these Terms or this Web Tool.

GENERAL

Any reference included in this Web Tool to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, NREL, or Alliance. The views and opinions expressed on the Web Tool or in any information or data available via the Web Tool do not necessarily represent the views of the U.S. Government or Alliance.

Unless otherwise specified, the Web Tool and any information or data available via the Web Tool are presented solely for use and access from within the United States, its territories, possessions, and protectorates. Alliance makes no representation or warranty of any kind that the Web Tool or any data available via the Web Tool is appropriate or available for use in other locations. If you access the Web Tool from a location other than the United States, you alone are responsible for compliance with any applicable local laws.

These Terms and any posted rules on the Web Tool constitute the entire agreement of the parties with respect to the subject matter hereof. No waiver by Alliance of any breach or default under these Terms will be deemed to be a waiver of any preceding or subsequent breach or default. These Terms will be binding upon and inure to the benefit of Alliance and its successors, trustees, and permitted assignees. Alliance may assign this agreement or any of its rights or obligations under these Terms with or without notice to you.

stripe

Get started quickly
Integrate with developer-friendly APIs or choose low-code or pre-built solutions.

Support any business model
E-commerce, subscriptions, SaaS platforms, marketplaces, and more—all within a unified platform.

Join millions of businesses
Stripe is trusted by ambitious startups and enterprises of every size.

Create your Stripe account

Email

Full name

Country

United States

Password

Create account

Have an account? Sign in

stripe

Stripe Connected Account Agreement

Last modified: August 22, 2022

Thank you for using Stripe Connect!

This agreement governs Connected Accounts' use of Stripe Connect Services, and describes how Connected Accounts and their third-party platform provider(s) may use the Stripe Connect Services.

This Stripe Connected Account Agreement ("**Connected Account Agreement**") forms a legal agreement between Stripe, Inc. ("**Stripe**") and the entity or sole proprietor on whose behalf a Stripe account is created ("**you**" and "**your**"), which Stripe account is intended to be integrated with a third-party platform provider that uses Stripe Connect Services ("**Stripe Connect Platform**"). The Stripe Services Agreement is incorporated into this Connected Account Agreement by this reference. Capitalized terms not defined in this Connected Account Agreement (either inline or by hyperlink), are defined in the Stripe Services Agreement. To the extent that there is a conflict between the Stripe Services Agreement and this Connected Account Agreement related to your use of the Stripe Connect Services, this Connected Account Agreement will prevail.

Non-applicability. Stripe Connect Platforms may use Stripe Connect to direct Stripe to send funds to Connected Accounts, for example, as payment for the Connected Accounts' goods or services that were provided to the Stripe Connect Platform. **If you receive payments of this kind, you are not using the Stripe services, and this Connected Account Agreement does not apply to you.** Also, you must contact the Stripe Connect Platform, not Stripe, with all questions you have about the status of these funds.

You and Stripe agree as follows:

1. Key Definitions.

The following terms are defined in the Stripe Services Agreement, but are repeated below for your convenience (you are a Platform User and Connected Account as the Stripe Services Agreement defines those terms):

"**Activity**" means any action taken on or related to a Connected Account that a Stripe Connect Platform or a Connected Account initiates, submits or performs, either through the Stripe Technology or through the Stripe Connect Services, including communication regarding the Services as related to that Connected Account.

"**Platform Services**" means the products and services that Platform Users receive from a Stripe Connect Platform, regardless of whether fees are charged (e.g., web development, customer support or hosting services).

"**Platform Provider Agreement**" means, as to each Connected Account, collectively, the agreements that a Stripe Connect Platform has with that Connected Account.

2. Your Stripe Account.

Stripe Connect Platforms can help you use the Services, which may include the Stripe Payments Services. A Stripe Connect Platform may help you to create your Stripe Account, or integrate your existing Stripe Account with the Stripe Connect Platform. A Stripe Connect Platform may conduct Activity on your behalf, as long as it does so according to your Platform Provider Agreement. Activity may be submitted, initiated or performed through the Stripe Dashboard or through the Stripe API, and this includes the communication of information about Transactions (if applicable), as well as other features as described in the Documentation. A Stripe Connect Platform may restrict your ability to (a) disconnect your Stripe Account from the Stripe Connect Platform; and (b) view, access or activate certain Services as long as in each case it does so according to your Platform Provider Agreement. You should read your Platform Provider Agreement carefully to understand the nature of the Platform Services and the Activity that a Stripe Connect Platform may conduct on your behalf. Stripe is not a Stripe Connect Platform, and only provides the Services described in this Connected Account Agreement and the Stripe Services Agreement.

3. Representation and Warranty; Your Responsibilities.

You represent as of the Effective Date, and warrant at all times during the Term, that the information that you provide to Stripe directly or through a Stripe Connect Platform is accurate and complete. You are solely responsible for, and Stripe disclaims all liability for, the provision of goods and services sold to your Customers as part of your use of the Services, and any obligations you may owe to your Customers. If you use the Stripe Payments Services, you are always financially liable to Stripe for the full amount of all Disputes (including chargebacks), Refunds, and fines that arise from your use of the Stripe Payments Services, regardless of whether you have agreed to share this liability with a Stripe Connect Platform. These obligations are described in more detail in the Stripe Services Agreement.

4. Stripe Dashboard.

Depending on how the Stripe Connect Platform has implemented the Stripe Connect Services, you may be able to directly manage your Stripe Account through the Stripe Dashboard. If you are able to access the Stripe Dashboard, you are responsible for all actions taken on your Stripe Account through the Stripe Dashboard. If you do not have access to the Stripe Dashboard, you must contact the Stripe Connect Platform if you need support or have any questions relating to the Services, this Connected Account Agreement or the Stripe Services Agreement.

5. Relationship to Stripe Connect Platforms.

5.1 Your Data.

Stripe Connect Platforms and Stripe may share data about you, Activity on your Stripe Account, and your Transactions ("**Your Data**") to facilitate your use of the Stripe Connect Services and the Platform Services. Where Stripe receives Your Data from Stripe Connect Platforms, Stripe may use the Data as allowed under this Section 5.1, the Stripe Services Agreement and the Stripe Privacy Policy.

5.2 Pricing and Fees.

Stripe's standard Fees for the Services are posted on the Stripe Pricing Page; but Stripe may have agreed to Fees with a Stripe Connect Platform that are different from these Fees. Stripe's Fees will either be disclosed to you separately or will be consolidated with the fees for the Platform Services. Stripe does not control and is not responsible for fees imposed by a Stripe Connect Platform, which should be made clear to you in your Platform Provider Agreement. At the Stripe Connect Platform's request, Stripe may deduct from your Stripe Account balance both Stripe's Fees and the fees for Platform Services the Stripe Connect Platform specifies to Stripe.

6. Disclaimer; Limitations on Stripe's Liability.

Stripe is not responsible for, and disclaims all liability arising from or relating to:

(a) any Stripe Connect Platform's acts or omissions in providing services to you or your customers, or for any Stripe Connect Platform's failure to comply with the terms of your Platform Provider Agreement;

(b) your obligations to your customers (including to properly describe and deliver the goods or services being sold to your customers); or

(c) your compliance with Laws and obligations related to your provision of goods or services to your customers, or receipt of charitable donations, including any obligation to provide customer service, notify and handle refunds or consumer complaints, provide receipts, register your legal entity, and other actions not related to the Services.

This section is in addition to, and does not limit, the provisions of the Stripe Services Agreement that disclaim or limit Stripe's liability.

7. Other General Legal Terms.

7.1 Term, Termination, and the Effects of Termination.

(a) The term of this Connected Account Agreement begins when you register your Stripe Account with a Stripe Connect Platform and continues until you or Stripe terminate this Connected Account Agreement under this Section. You may terminate this Connected Account Agreement by deregistering your Stripe Account from all Stripe Connect Platforms. If after termination you register your Stripe Account with a Stripe Connect Platform again, this Agreement will apply starting on the date on which you register your Stripe Account with a Stripe Connect Platform again. Stripe may terminate this Connected Account Agreement at any time for any reason by notifying you.

(b) Terminating this Connected Account Agreement will not immediately terminate the Stripe Services Agreement. Stripe and you may only terminate the Stripe Services Agreement according to its terms. This Connected Account Agreement will automatically terminate if the Stripe Services Agreement terminates.

7.2 Stripe Services Agreement - Version.

The Stripe Services Agreement version incorporated into this Connected Account Agreement is the version that applies to your Stripe Account jurisdiction. If the name of your jurisdiction does not appear in the title of the page accessible via this Stripe Services Agreement link, please contact Stripe to obtain the correct link.

stripe

Stripe Services Agreement — United States

On this page

Welcome to Stripe!

This Stripe Services Agreement includes this introduction, the General Terms, Definitions, Services Terms, and incorporated documents and terms ("**Agreement**") and forms a legal agreement between Stripe, Inc. ("**Stripe**") and the entity or sole proprietor on whose behalf a Stripe account is created ("**you**" and "**your**") to receive certain payment processing, data, technology and analytics, or other business services offered by Stripe and its Affiliates. This Agreement states the terms and conditions that apply to your use of the Services.

This Agreement is effective upon the date you first access or use the Services ("**Effective Date**") and continues until you or Stripe terminates it (this period, the "**Term**"). Capitalized terms used in this Agreement that are not defined inline are defined in the Definitions.

As referenced in Section 13 of the General Terms, any dispute between you and Stripe is subject to a class action waiver and must be resolved by individual binding arbitration. Please read the arbitration provision in this Agreement as it affects your rights under this Agreement.

General Terms

Last modified: August 22, 2022

You and Stripe agree as follows:

1. Your Stripe Account.

1.1 Eligibility.

Only businesses (including sole proprietors) and non-profit organizations located in the United States are eligible to apply for a Stripe Account and use the Services. Stripe and its Affiliates may provide Services to you or your Affiliates in other

countries or regions under separate agreements. You and your Representative must not attempt to create a Stripe Account on behalf of or for the benefit of a user whose use of the Stripe services was suspended or terminated by Stripe, unless Stripe approves otherwise.

1.2 Business Representative.

You and your Representative individually affirm to Stripe that (a) your Representative is authorized to provide User Information on your behalf and to bind you to this Agreement; and (b) your Representative is an executive officer, senior manager or otherwise has significant responsibility for the control, management or direction of your business. Stripe may require you or your Representative to provide additional information or documentation demonstrating your Representative's authority.

1.3 Sole Proprietors.

If you are a sole proprietor, you and your Representative also affirm that your Representative is personally responsible and liable for your use of the Services and your obligations to Customers, including payment of amounts you owe under this Agreement.

1.4 Age Requirements.

If you are a sole proprietor, and you are not old enough to enter into a contract on your own behalf (which is commonly but not always 18 years old), but you are 13 years old or older, your Representative must be your parent or legal guardian. If you are a legal entity that is owned, directly or indirectly, by an individual who is not old enough to enter into a contract on their own behalf, but the individual is 13 years old or older, your Representative must obtain the consent of either your board or an authorized officer. The approving board, authorized officer, parent or legal guardian is responsible to Stripe and is legally bound to this Agreement as if it had agreed to this Agreement itself. You must not use the Services if you are under 13 years of age.

2. Services and Support.

2.1 Services.

Stripe (and its Affiliates, as applicable) will make available to you the Services, including those described in the applicable Services Terms, and, if applicable, give you access to a Stripe Dashboard.

2.2 Services Terms; Order of Precedence.

The Services Terms contain specific terms governing the parties' rights and obligations related to the Services described in those Services Terms. If there are no Services Terms for a particular Stripe service, then only these General Terms govern. By accessing or using a Service, you agree to comply with the applicable Services Terms. If any term in these General Terms conflicts with a term in any Services Terms or set of terms incorporated by reference into this Agreement, then unless terms of lower precedence expressly state to the contrary, the order of precedence is: (a) the Services Terms; (b) these General Terms; and (c) all terms incorporated by reference into this Agreement. Your access to or use of the Services may also be subject to additional terms to which you agree through the Stripe Dashboard.

2.3 Service Modifications and Updates.

Stripe may modify the Services and Stripe Technology at any time, including adding or removing functionality or imposing conditions on use of the Services. Stripe will notify you of material adverse changes in, deprecations to, or removal of functionality from, Services or Stripe Technology that you are using. Stripe is not obligated to provide any

Updates. However, if Stripe makes an Update available, you must fully install the Update by the date or within the time period stated in Stripe's notice; or, if there is no date or period stated in the notice, then no later than 30 days after the date of the notice.

2.4 Subcontracting.

Stripe may subcontract its obligations under this Agreement to third parties.

2.5 Services Restrictions.

You may only use the Services for business purposes. You must not, and must not enable or allow any third party to:

(a) use the Services for personal, family or household purposes;

(b) act as service bureau or pass-through agent for the Services with no added value to Customers;

(c) work around any of the technical limitations of the Services or enable functionality that is disabled or prohibited, or access or attempt to access non-public Stripe systems, programs, data, or services;

(d) except as Law permits, reverse engineer or attempt to reverse engineer the Services or Stripe Technology;

(e) use the Services to engage in any activity that is illegal, fraudulent, deceptive or harmful;

(f) perform or attempt to perform any action that interferes with the normal operation of the Services or affects other Stripe users' use of Stripe services; or

(g) copy, reproduce, republish, upload, post, transmit, resell, or distribute in any way, any part of the Services, Documentation, or the Stripe Website except as permitted by Law.

2.6 Beta Services.

(a) *Classification*. Stripe may classify certain Stripe services or Stripe Technology, including a particular release or feature, as Beta. A Stripe service may be generally available in some circumstances (e.g., in some countries or regions) while still classified as Beta in other circumstances.

(b) *Nature of Beta Services*. By their nature, Beta Services may be feature-incomplete or contain bugs. Stripe may describe limitations that exist within a Beta Service; however, your reliance on the accuracy or completeness of these descriptions is at your own risk. You should not use Beta Services in a production environment until and unless you understand and accept the limitations and flaws that may be present in the Beta Services.

(c) *Feedback*. Unless Stripe otherwise agrees in writing, your use of Beta Services is confidential, and you must provide timely Feedback on the Beta Services in response to Stripe requests.

(d) *Availability During Beta Period*. Stripe may suspend or terminate your access to any Beta Services at any time.

2.7 Support.

Stripe will provide you with support to resolve general issues relating to your Stripe Account and your use of the Services through resources and documentation that Stripe makes available on the Stripe Website and in the Documentation. Stripe's support is also available by contacting Stripe at **contact us**. Stripe is not responsible for providing support to Customers.

2.8 Third-Party Services.

Stripe may reference, enable you to access, or promote (including on the Stripe Website) Third-Party Services. These Third-Party Services are provided for your convenience only and Stripe does not approve, endorse, or recommend any Third-Party Services to you. **Your access and use of any Third-Party Service is at your own risk and Stripe disclaims all responsibility and liability for your use of any Third-Party Service. Third-Party Services are not Services and are not governed by this Agreement or Stripe's Privacy Policy. Your use of any Third-Party Service, including those linked from the Stripe Website, is subject to that Third-Party Service's own terms of use and privacy policies (if any).**

3. Information; Your Business.

3.1 User Information.

Upon Stripe's request, you must provide User Information to Stripe in a form satisfactory to Stripe. You must keep the User Information in your Stripe Account current. You must promptly update your Stripe Account with any changes affecting you, the nature of your business activities, your Representative, beneficial owners, principals, or any other pertinent information. You must immediately notify Stripe, and provide to Stripe updated User Information, if (a) you experience or anticipate experiencing a Change of Control; (b) you experience or anticipate experiencing a material change in your business or financial condition, including if you experience or are likely to experience an Insolvency Proceeding; (c) the regulatory status of the business for which you are using the Services changes, including if it becomes subject, or no longer subject, to regulatory oversight; or (d) a Governmental Authority has notified you that you or your business is the subject of investigative action.

3.2 Information Retrieved by Stripe.

You authorize Stripe to retrieve information about you and your business from Stripe's service providers and other third parties, including credit reporting agencies, banking partners and information bureaus, and you authorize and direct those third parties to compile and provide that information to Stripe. This information may include your, or your Representative's, name, addresses, credit history, banking relationships, and financial history.

4. Services Fees; Taxes.

4.1 Services Fees.

The Fees are stated on the Stripe Pricing Page, unless you and Stripe otherwise agree in writing. Stripe may revise the Fees at any time. If Stripe revises the Fees for a Service that you are currently using, Stripe will notify you at least 30 days before the revised Fees apply to you.

4.2 Collection of Fees and Other Amounts.

You must pay, or ensure that Stripe is able to collect, Fees and other amounts you owe under this Agreement when due. Stripe may deduct, recoup or setoff Fees and other amounts you owe under this Agreement, or under any other agreements you have with Stripe or any of its Affiliates, from your Stripe Account balance, or invoice you for those amounts. If you fail to pay invoiced amounts when due, if your Stripe Account balance is negative or does not contain funds sufficient to pay amounts that you owe under this Agreement, or under any other agreement with Stripe or any of its Affiliates, or if Stripe is unable to collect amounts due from your Stripe Account balance, then Stripe may, to the extent Law permits, deduct, recoup or setoff those amounts from: (a) if established and applicable, each Reserve; (b) funds payable by Stripe or its Affiliate to you or your Affiliate; (c) if established, each User Affiliate Reserve; (d) each User Bank

Account; and (e) the Stripe account balance of each Stripe account that Stripe determines, acting reasonably, is associated with you or your Affiliate. If the currency of the amount being deducted is different from the currency of the amount you owe, Stripe may deduct, recoup or setoff an amount equal to the amount owed (using Stripe's conversion rate) together with any fees Stripe incurs in making the conversion.

4.3 Debit Authorization.

Without limiting Section 4.2, you authorize Stripe to debit each User Bank Account without separate notice, and according to the applicable **User Bank Account Debit Authorization**, to collect amounts you owe under this Agreement. If Stripe is unable to collect those amounts by debiting a User Bank Account, then you immediately grant to Stripe a new, original authorization to debit each User Bank Account without notice and according to the applicable **User Bank Account Debit Authorization**. Stripe may rely on this authorization to make one or more attempts to collect all or a subset of the amounts owed. Your authorization under this Section 4.3 will remain in full force and effect until (a) all of your Stripe Accounts are closed; or (b) all fees and other amounts you owe under this Agreement are paid, whichever occurs later. If applicable debit scheme authorization rules grant you the right to revoke your debit authorization, then to the extent Law permits, you waive that right.

4.4 Taxes.

Stripe's fees exclude all Taxes, except as the Stripe Pricing Page states to the contrary. You have sole responsibility and liability for:

(a) determining which, if any, Taxes or fees apply to the sale of your products and services, acceptance of donations, or payments you make or receive in connection with your use of the Services; and

(b) assessing, collecting, reporting and remitting Taxes for your business.
If Stripe is required to withhold any Taxes, Stripe may deduct those Taxes from amounts otherwise owed to you and pay those Taxes to the appropriate taxing authority. If you are exempt from paying, or are otherwise eligible to pay a reduced rate on, those Taxes, you may provide to Stripe an original certificate that satisfies applicable legal requirements attesting to your tax-exempt status or reduced rate eligibility, in which case Stripe will not deduct the Taxes covered by the certificate. You must provide accurate information regarding your tax affairs as Stripe reasonably requests, and must promptly notify Stripe if any information that Stripe prepopulates is inaccurate or incomplete. Stripe may send documents to you and taxing authorities for transactions processed using the Services. Specifically, Law may require Stripe to file periodic informational returns with taxing authorities related to your use of the Services. Stripe may send tax-related information electronically to you.

5. User Bank Accounts; Funds.

5.1 User Bank Accounts; Prohibition on Grant or Assignment.

You must designate at least one User Bank Account in connection with the Services. Stripe may debit and credit a User Bank Account as described in this Agreement. You must not grant or assign to any third party any lien on or interest in funds that may be owed to you under this Agreement until the funds are deposited into a User Bank Account.

5.2 Investment of Funds.

To the extent Law and the applicable Financial Services Terms permit, Stripe and its Affiliates may invest the funds that they hold into liquid investments. Stripe or its applicable Affiliate owns the earnings from these investments. You irrevocably assign to Stripe or its applicable Affiliate all rights you have (if any) to earnings from these investments.

5.3 Regulated Money Transmission; Stripe Status.

Certain Services involve regulated money transmission under U.S. Law. To the extent that your use of the Services involves money transmission or other regulated services under U.S. Law, Stripe's Affiliate, SPC, provides those regulated Services, and the SPC terms located on or accessible from the Stripe Legal Page will apply to you, unless the applicable Services Terms specify otherwise. Stripe is not a bank, and does not accept deposits.

5.4 Dormant Accounts.

If you leave any funds dormant in a Stripe Account and you do not instruct Stripe on where to send them, Stripe may deem the funds abandoned by you and deliver them to the appropriate Governmental Authority. However, if Law requires, Stripe will attempt to notify you before doing so.

6. Termination; Suspension; Survival.

6.1 Termination.

(a) *Your Termination*. You may terminate this Agreement at any time by closing your Stripe Account. To do so, you must open **the account information tab in your account settings**, select "close my account" and stop using the Services. If after termination you use the Services again, this Agreement will apply with an Effective Date that is the date on which you first use the Services again.

(b) *Stripe Termination*. Stripe may terminate this Agreement (or any part) or close your Stripe Account at any time for any or no reason (including if any event listed in Sections 6.2(a)–(i) of these General Terms occurs) by notifying you. In addition, Stripe may terminate this Agreement (or relevant part) for cause if Stripe exercises its right to suspend Services (including under Section 6.2 of these General Terms) and does not reinstate the suspended Services within 30 days.

(c) *Termination for Material Breach*. A party may terminate this Agreement immediately upon notice to the other party if the other party materially breaches this Agreement, and if capable of cure, does not cure the breach within 10 days after receiving notice specifying the breach. If the material breach affects only certain Services, the non-breaching party may choose to terminate only the affected Services.

(d) *Effect on Other Agreements*. Unless stated to the contrary, termination of this Agreement will not affect any other agreement between the parties or their Affiliates.

6.2 Suspension.

Stripe may immediately suspend providing any or all Services to you, and your access to the Stripe Technology, if:

(a) Stripe believes it will violate any Law, Financial Services Terms or Governmental Authority requirement;

(b) a Governmental Authority or a Financial Partner requires or directs Stripe to do so;

(c) you do not update in a timely manner your implementation of the Services or Stripe Technology to the latest production version Stripe recommends or requires;

(d) you do not respond in a timely manner to Stripe's request for User Information or do not provide Stripe adequate time to verify and process updated User Information;

(e) you breach this Agreement or any other agreement between the parties;

(f) you breach any Financial Services Terms;

(g) you enter an Insolvency Proceeding;

(h) Stripe believes that you are engaged in a business, trading practice or other activity that presents an unacceptable risk to Stripe; or

(i) Stripe believes that your use of the Services (i) is or may be harmful to Stripe or any third party; (ii) presents an unacceptable level of credit risk; (iii) increases, or may increase, the rate of fraud that Stripe observes; (iv) degrades, or may degrade, the security, stability or reliability of the Stripe services, Stripe Technology or any third party's system (e.g., your involvement in a distributed denial of service attack); (v) enables or facilitates, or may enable or facilitate, illegal or prohibited transactions; or (vi) is or may be unlawful.

6.3 Survival.

The following will survive termination of this Agreement:

(a) provisions that by their nature are intended to survive termination (including Sections 4, 7.2, 9.4, 11, 12 and 13 of these General Terms); and

(b) provisions that allocate risk, or limit or exclude a party's liability, to the extent necessary to ensure that a party's potential liability for acts and omissions that occur during the Term remains unchanged after this Agreement terminates.

7. Use Rights.

7.1 Use of Services.

Subject to the terms of this Agreement, Stripe grants you a worldwide, non-exclusive, non-transferable, non-sublicensable, royalty-free license during the Term to access the Documentation, and access and use the Stripe Technology, as long as your access and use is (a) solely as necessary to use the Services; (b) solely for your business purposes; and (c) in compliance with this Agreement and the Documentation.

7.2 Feedback.

During the Term, you and your Affiliates may provide Feedback to Stripe or its Affiliates. You grant, on behalf of yourself and your Affiliates, to Stripe and its Affiliates a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to exploit that Feedback for any purpose, including developing, improving, manufacturing, promoting, selling and maintaining the Stripe services. All Feedback is Stripe's confidential information.

7.3 Marks Usage.

Subject to the terms of this Agreement, each party grants to the other party and its Affiliates a worldwide, non-exclusive, non-transferable, non-sublicensable, royalty-free license during the Term to use the Marks of the grantor party or its Affiliate solely to identify Stripe as your service provider. Accordingly, Stripe and its Affiliates may use those Marks:

(a) on Stripe webpages and apps that identify Stripe's customers;

(b) in Stripe sales/marketing materials and communications; and

(c) in connection with promotional activities to which the parties agree in writing.

When using Marks of Stripe or its Affiliate, you must comply with the **Stripe Marks Usage Terms** and all additional usage terms and guidelines that Stripe provides to you in writing (if any). All goodwill generated from the use of Marks will inure to the sole benefit of the Mark owner.

7.4 No Joint Development; Reservation of Rights.

Any joint development between the parties will require and be subject to a separate agreement between the parties. Nothing in this Agreement assigns or transfers ownership of any IP Rights to the other party. All rights (including IP Rights) not expressly granted in this Agreement are reserved.

8. Privacy and Data Use.

8.1 Privacy Policies.

Each party will make available a Privacy Policy that complies with Law. Stripe's **Privacy Policy** explains how and for what purposes Stripe collects, uses, retains, discloses and safeguards the Personal Data you provide to Stripe.

8.2 Personal Data.

When you provide Personal Data to Stripe, or authorize Stripe to collect Personal Data, you must provide all necessary notices to and obtain all necessary rights and consents from the applicable individuals (including your Customers) sufficient to enable Stripe to lawfully collect, use, retain and disclose the Personal Data in the ways this Agreement and Stripe's **Privacy Policy** describe. Stripe will not sell or lease Personal Data that Stripe receives from you to any third party.

8.3 Protected Data.

To the extent Law permits, Stripe will use Protected Data to (a) secure, provide, provide access to, and update the Stripe services; (b) fulfill its obligations under Law, and comply with Financial Partner and Governmental Authority requirements and requests; and (c) prevent and mitigate fraud, financial loss, and other harm. Stripe is not obligated to retain Protected Data after the Term, except as (w) required by Law; (x) required for Stripe to perform any post-termination obligations; (y) this Agreement otherwise states; or (z) the parties otherwise agree in writing. You are responsible for being aware of and complying with Law governing your use, storage and disclosure of Protected Data.

8.4 Stripe Data.

You may use the Stripe Data only as this Agreement and other agreements between Stripe and you (or their Affiliates) permit.

8.5 Data Processing Agreement.

The **Data Processing Agreement**, including the Approved Data Transfer Mechanisms (as defined in the Data Processing Agreement) that apply to your use of the Services and transfer of Personal Data, is incorporated into this Agreement by this reference. Each party will comply with the terms of the Data Processing Agreement.

8.6 Use of Fraud Signals.

If Stripe provides you with information regarding the possibility or likelihood that a transaction may be fraudulent or that an individual cannot be verified, Stripe may incorporate your subsequent actions and inactions into Stripe's fraud and verification model, for the purpose of identifying future potential fraud. Please see the **Stripe Privacy Center** for more information on **Stripe's collection of end-customer data** for this purpose and for **guidance on how to notify your Customers**.

9. Data Security.

9.1 Controls.

Each party will maintain commercially reasonable administrative, technical, and physical controls designed to protect data in its possession or under its control from unauthorized access, accidental loss and unauthorized modification. You are responsible for implementing administrative, technical, and physical controls that are appropriate for your business.

9.2 PCI-DSS.

Stripe will make reasonable efforts to provide the Services in a manner consistent with PCI-DSS requirements that apply to Stripe.

9.3 Stripe Account Credentials.

You must prevent any Credential Compromise, and otherwise ensure that your Stripe Account is not used or modified by anyone other than you and your representatives. If a Credential Compromise occurs, you must promptly notify and cooperate with Stripe, including by providing information that Stripe requests. Any act or failure to act by Stripe will not diminish your responsibility for Credential Compromises.

9.4 Data Breach.

You must notify Stripe immediately if you become aware of an unauthorized acquisition, modification, disclosure, access to, or loss of Personal Data on your systems.

9.5 Audit Rights.

If Stripe believes that a compromise of data has occurred on your systems, website, or app, Stripe may require you to permit a Stripe approved third-party auditor to audit the security of your systems and facilities. You must fully cooperate with all auditor requests for information or assistance. As between the parties, you are responsible for all costs and expenses associated with these audits. Stripe may share with Financial Services Partners any report the auditor issues.

10. Representations and Warranties.

10.1 Representations and Warranties.

You represent as of the Effective Date, and warrant at all times during the Term, that:

(a) you have the right, power, and ability to enter into and perform under this Agreement;

(b) you are a business (which may be a sole proprietor) or a non-profit organization located in the United States and are eligible to apply for a Stripe account and use the Services;

(c) you have, and comply with, all necessary rights, consents, licenses, and approvals for the operation of your business and to allow you to access and use the Services in compliance with this Agreement and Law;

(d) your employees, contractors and agents are acting consistently with this Agreement;

(e) your use of the Services does not violate or infringe upon any third-party rights, including IP Rights, and you have obtained, as applicable, all necessary rights and permissions to enable your use of Content in connection with the Services;

(f) you are authorized to initiate settlements to and debits from the User Bank Accounts;

(g) you comply with Law with respect to your business, your use of the Services and Stripe Technology, and the performance of your obligations in this Agreement;

(h) you comply with the Documentation;

(i) you comply with the Financial Services Terms, and are not engaging in activity that any Financial Partner identifies as damaging to its brand;

(j) you do not use the Services to conduct a Restricted Business, transact with any Restricted Business, or enable any individual or entity (including you) to benefit from any Restricted Business;

(k) you own each User Bank Account, and each User Bank Account is located in a Stripe-approved country for the location of your Stripe Account, as described in the Documentation; and

(l) all information you provide to Stripe, including the User Information, is accurate and complete.

10.2 Scope of Application.

Unless this Agreement states to the contrary elsewhere, the representations and warranties in Sections 10.1 and 15.9 of these General Terms apply generally to your performance under this Agreement. Additional representations and warranties that apply only to a specific Service may be included in the Services Terms.

11. Indemnity.

11.1 Stripe IP Infringement.

(a) *Defense and Indemnification*. Stripe will defend you against any IP Claim and indemnify you against all IP Claim Losses.

(b) *Limitations*. Stripe's obligations in this Section 11.1 do not apply if the allegations do not specify that the Stripe Technology, Services, or Mark of Stripe or its Affiliate is the basis of the IP Claim, or to the extent the IP Claim or IP Claim Losses arise out of:

(i) the use of the Stripe Technology or Services in combination with software, hardware, data, or processes not provided by Stripe;

(ii) failure to implement, maintain and use the Stripe Technology or Services in accordance with the Documentation and this Agreement;

(iii) your breach of this Agreement; or

(iv) your negligence, fraud or willful misconduct.

(c) *Process*. You must promptly notify Stripe of the IP Claim for which you seek indemnification; however, any delay or failure to notify will not relieve Stripe of its obligations under this Section 11, except to the extent Stripe has been prejudiced by the delay or failure. You must give Stripe sole control and authority to defend and settle the IP Claim, but (i) you may participate in the defense and settlement of the IP Claim with counsel of your own choosing at your own expense; and (ii) Stripe will not enter into any settlement that imposes any obligation on you (other than payment of money, which Stripe will pay) without your consent. You must reasonably assist Stripe in defending the IP Claim.

(d) *Other Stripe Actions*. Stripe may in its discretion and at no additional expense to you:

(i) modify the Stripe Technology or Services so that they are no longer claimed to infringe or misappropriate IP Rights of a third party;

(ii) replace the affected Stripe Technology or Services with a non-infringing alternative;

(iii) obtain a license for you to continue to use the affected Stripe Technology, Services, or Mark; or

(iv) terminate your use of the affected Stripe Technology, Services, or Mark upon 30 days' notice.

(e) ***Exclusive Remedy*. This Section 11.1 states Stripe's sole liability, and your sole and exclusive right and remedy, for infringement by the Stripe Technology, Services, or Marks of Stripe or its Affiliate, including any IP Claim.**

11.2 User Indemnification.

(a) *Defense*. You will defend the Stripe Parties against any Claim made against any of the Stripe Parties to the extent arising out of or relating to:

(i) your breach of any of your representations, warranties or obligations under this Agreement;

(ii) your use of the Services, including use of Personal Data;

(iii) an allegation that any of the Marks you license to Stripe, or your Content, infringes on or misappropriates the rights, including IP Rights, of the third party making the Claim; or

(iv) a User Party's negligence, willful misconduct or fraud.

(b) *Indemnification*. You will indemnify the Stripe Parties against all Stripe Losses arising out of or relating to Claims described in this Section 11.2.

12. Disclaimer and Limitations on Liability.

The following disclaimer and limitations will apply notwithstanding the failure of the essential purpose of any limited remedy.

12.1 Disclaimer.

Stripe provides the Services and Stripe Technology "AS IS" and "AS AVAILABLE". Except as expressly stated as a "warranty" in this Agreement, and to the maximum extent permitted by Law, Stripe does not make any, and expressly disclaims all, express and implied warranties and statutory guarantees with respect to its performance under this Agreement, the Services, Financial Partners, the Stripe Technology, Stripe Data and the Documentation, including as related to availability, the implied warranties of fitness for a particular purpose, merchantability and non-infringement, and the implied warranties arising out of any course of dealing, course of performance or usage in trade. The Stripe Parties are not liable for any losses, damages, or costs that you or others may suffer arising out of or relating to hacking, tampering, or other unauthorized access or use of the Services, your Stripe Account, or Protected Data, or your failure to use or implement anti-fraud or data security measures. Further, the Stripe Parties are not liable for any losses, damages, or costs that you or others may suffer arising out of or relating to (a) your access to, or use of, the Services in a way that is inconsistent with this Agreement or the Documentation; (b) unauthorized access to servers or infrastructure, or to Stripe Data or Protected Data; (c) Service interruptions or stoppages; (d) bugs, viruses, or other harmful code that may be transmitted to or through the Service (e) errors, inaccuracies, omissions or losses in or to any Protected Data or Stripe Data; (f) Content; or (g) the defamatory, offensive, or illegal conduct of others.

12.2 LIMITATIONS ON LIABILITY.

(a) ***Indirect Damages*. To the maximum extent permitted by Law, the Stripe Parties will not be liable to you or your Affiliates in relation to this Agreement or the Services during and after the Term, whether in contract, negligence, strict liability, tort or other legal or equitable theory, for any lost profits, personal injury, property damage, loss of data, business interruption, indirect, incidental, consequential, exemplary, special, reliance, or punitive damages, even if these losses, damages, or costs are foreseeable, and whether or not you or the Stripe Parties have been advised of their possibility.**

(b) ***General Damages*. To the maximum extent permitted by Law, the Stripe Parties will not be liable to you or your Affiliates in relation to this Agreement or the Services during and after the Term, whether in contract, negligence, strict liability, tort or other legal or equitable theory, for losses, damages, or costs exceeding in the aggregate the greater of (i) the total amount of Fees you paid to Stripe (excluding all pass-through fees levied by Financial Partners) during the 3-month period immediately preceding the event giving rise to the liability; and (ii) $500 USD.**

13. Dispute Resolution; Agreement to Arbitrate.

13.1 Binding Arbitration.

(a) All disputes, claims and controversies, whether based on past, present or future events, arising out of or relating to statutory or common law claims, the breach, termination, enforcement, interpretation or validity of any provision of this Agreement, and the determination of the scope or applicability of your agreement to arbitrate any dispute, claim or controversy originating from this Agreement, but specifically excluding any dispute principally related to either party's IP Rights (which will be resolved in litigation before the United States District Court for the Northern District of California), will be determined by binding arbitration in San Francisco, California before a single arbitrator.

(b) The American Arbitration Association will administrate the arbitration under its Commercial Arbitration Rules. The Expedited Procedures of the American Arbitration Association's Commercial Arbitration Rules will apply for cases in which no disclosed claim or counterclaim exceeds $75,000 USD (excluding interest, attorneys' fees and arbitration fees and costs). Where no party's claim exceeds $25,000 USD (excluding interest, attorneys' fees and arbitration fees and costs), and in other cases where the parties agree, Section E-6 of the Expedited Procedures of the American Arbitration Association's Commercial Arbitration Rules will apply.

(c) The arbitrator will apply the substantive law of the State of California and of the United States, excluding their conflict or choice of law rules.

(d) Nothing in this Agreement will preclude the parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

(e) The parties acknowledge that this Agreement evidences a transaction involving interstate commerce. Notwithstanding the provisions in this Section 13 referencing applicable substantive law, the Federal Arbitration Act (9 U.S.C. Sections 1-16) will govern any arbitration conducted in accordance with this Agreement.

13.2 Arbitration Procedure.

(a) A party must notify the other party of its intent to commence arbitration prior to commencing arbitration. The notice must specify the date on which the arbitration demand is intended to be filed, which must be at least 30 days after the date of the notice. During this time period, the parties will meet for the purpose of resolving the dispute prior to commencing arbitration.

(b) Subject to Section 13.2(a), each party may commence arbitration by providing to the American Arbitration Association and the other party to the dispute a written demand for arbitration, stating the subject of the dispute and the relief requested.

(c) Subject to the disclaimers and limitations of liability stated in this Agreement, the appointed arbitrators may award monetary damages and any other remedies allowed by the laws of the State of California. In making a determination, the arbitrator will not have the authority to modify any term of this Agreement. The arbitrator will deliver a reasoned, written decision with respect to the dispute to each party, who will promptly act in accordance with the arbitrator's decision. Any award (including interim or final remedies) may be confirmed in or enforced by a state or federal court located in San Francisco, California. The decision of the arbitrator will be final and binding on the parties, and will not be subject to appeal or review.

(d) In accordance with the AAA Rules, the party initiating the arbitration is responsible for paying the applicable filing fee. Each party will advance one-half of the fees and expenses of the arbitrator, the costs of the attendance of the arbitration reporter at the arbitration hearing, and the costs of the arbitration facility. In any arbitration arising out of or relating to this Agreement, the arbitrator will award to the prevailing party, if any, the costs and attorneys' fees reasonably incurred by the prevailing party in connection with those aspects of its claims or defenses on which it prevails, and any opposing awards of costs and legal fees awards will be offset.

13.3 Confidentiality.

The parties will keep confidential the existence of the arbitration, the arbitration proceeding, the hearing and the arbitrator's decision, except (a) as necessary to prepare for and conduct the arbitration hearing on the merits; (b) in connection with a court application for a preliminary remedy, or confirmation of an arbitrator's decision or its enforcement; (c) Stripe may disclose the arbitrator's decision in confidential settlement negotiations; (d) each party may disclose as necessary to professional advisors that are subject to a strict duty of confidentiality; and (e) as Law otherwise requires. The parties, witnesses, and arbitrator will treat as confidential and will not disclose to any third person (other than witnesses or experts) any documentary or other evidence produced in any arbitration, except as Law requires or if the evidence was obtained from the public domain or was otherwise obtained independently from the arbitration.

13.4 Conflict of Rules.

In the case of a conflict between the provisions of this Section 13 and the AAA Rules, the provisions of this Section 13 will prevail.

13.5 Class Waiver.

To the extent Law permits, any dispute arising out of or relating to this Agreement, whether in arbitration or in court, will be conducted only on an individual basis and not in a class, consolidated or representative action. Notwithstanding any other provision of this Agreement or the AAA Rules, disputes regarding the interpretation, applicability, or enforceability of this class waiver may be resolved only by a court and not by an arbitrator. If this waiver of class or consolidated actions is deemed invalid or unenforceable, neither party is entitled to arbitration.

13.6 No Jury Trial.

If for any reason a claim or dispute proceeds in court rather than through arbitration, each party knowingly and irrevocably waives any right to trial by jury in any action, proceeding or counterclaim arising out of or relating to this Agreement or any of the transactions contemplated between the parties.

14. Modifications to this Agreement.

Stripe may modify all or any part of this Agreement at any time by posting a revised version of the modified General Terms (including the introduction to this Agreement and the Definitions), Services Terms or terms incorporated by reference on the Stripe Legal Page or by notifying you. The modified Agreement is effective upon posting or, if Stripe notifies you, as stated in the notice. By continuing to use Services after the effective date of any modification to this Agreement, you agree to be bound by the modified Agreement. It is your responsibility to check the Stripe Legal Page regularly for modifications to this Agreement. Stripe last modified these General Terms on the date listed under the "General Terms" heading, and each set of Services Terms on the date listed under the heading for those terms. Except as this Agreement (including in this Section 14) otherwise allows, this Agreement may not be modified except in a writing signed by the parties.

15. General Provisions.

15.1 Electronic Communications.

By accepting this Agreement or using any Service, you consent to electronic communications as described in the **E-SIGN Disclosure**, which is incorporated into this Agreement by this reference.

15.2 Notices and Communications.

(a) *Notices to Stripe*. Unless this Agreement states otherwise, for notices to Stripe, you must **contact us**. A notice you send to Stripe is deemed to be received when Stripe receives it.

(b) *Communications to you*. In addition to sending you a Communication electronically as Section 15.1 of these General Terms describes, Stripe may send you Communications by physical mail or delivery service to the postal address listed in the applicable Stripe Account. A Communication Stripe sends to you is deemed received by you on the earliest of (i) when posted to the Stripe Website or Stripe Dashboard; (ii) when sent by text message or email; and (iii) three business days after being sent by physical mail or when delivered, if sent by delivery service.

15.3 Legal Process.

Stripe may respond to and comply with any Legal Process that Stripe believes to be valid. Stripe may deliver or hold any funds or, subject to the terms of Stripe's Privacy Policy, any data as required under the Legal Process, even if you are

receiving funds or data on behalf of other parties. Where Law permits, Stripe will notify you of the Legal Process by sending a copy to the email address in the applicable Stripe Account. Stripe is not responsible for any losses, whether direct or indirect, that you may incur as a result of Stripe's response or compliance with a Legal Process in accordance with this Section 15.3.

15.4 Collection Costs.

You are liable for all costs Stripe incurs during collection of any amounts you owe under this Agreement, in addition to the amounts you owe. Collection costs may include attorneys' fees and expenses, costs of any arbitration or court proceeding, collection agency fees, applicable interest, and any other related cost.

15.5 Interpretation.

(a) No provision of this Agreement will be construed against any party on the basis of that party being the drafter.

(b) References to "includes" or "including" not followed by "only" or a similar word mean "includes, without limitation" and "including, without limitation," respectively.

(c) Except where expressly stated otherwise in a writing executed between you and Stripe, this Agreement will prevail over any conflicting policy or agreement for the provision or use of the Services.

(d) All references in this Agreement to any terms, documents, Law or Financial Services Terms are to those items as they may be amended, supplemented or replaced from time to time. All references to APIs and URLs are references to those APIs and URLs as they may be updated or replaced.

(e) The section headings of this Agreement are for convenience only, and have no interpretive value.

(f) Unless expressly stated otherwise, any consent or approval that may be given by a party (i) is only effective if given in writing and in advance; and (ii) may be given or withheld in the party's sole and absolute discretion.

(g) References to "business days" means weekdays on which banks are generally open for business. Unless specified as business days, all references in this Agreement to days, months or years mean calendar days, calendar months or calendar years.

(h) Unless expressly stated to the contrary, when a party makes a decision or determination under this Agreement, that party has the right to use its sole discretion in making that decision or determination.

(i) The United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement.

15.6 Waivers.

To be effective, a waiver must be in a writing signed by the waiving party. The failure of either party to enforce any provision of this Agreement will not constitute a waiver of that party's rights to subsequently enforce the provision.

15.7 Force Majeure.

Stripe and its Affiliates will not be liable for any losses, damages, or costs you suffer, or delays in Stripe or its Affiliates' performance or non-performance, to the extent caused by a Force Majeure Event.

15.8 Assignment.

You may not assign or transfer any obligation or benefit under this Agreement without Stripe's consent. Any attempt to assign or transfer in violation of the previous sentence will be void in each instance. If you wish to assign this Agreement, please **contact us**. Stripe may, without your consent, freely assign and transfer this Agreement, including any of its rights or obligations under this Agreement. This Agreement will be binding on, inure to the benefit of, and be enforceable by the parties and their permitted assigns.

15.9 Export Control.

You must not use or otherwise export, re-export or transfer the Stripe Technology except as authorized by United States law and the laws of the jurisdiction(s) in which the Stripe Technology was distributed and obtained, including by providing access to Stripe Technology (a) to any individual or entity ordinarily resident in a High-Risk Jurisdiction; or (b) to any High-Risk Person. By using the Stripe Technology, you represent as of the Effective Date and warrant during the Term that you are not (x) located in or organized under the laws of any High-Risk Jurisdiction; (y) a High-Risk Person; or (z) owned 50% or more, or controlled, by individuals and entities (i) located in or, as applicable, organized under the laws of any High-Risk Jurisdiction; or (ii) any of whom or which is a High-Risk Person. You must not use the Stripe Technology for any purposes prohibited by Law, including the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

15.10 No Agency.

Each party to this Agreement, and each Financial Partner, is an independent contractor. Nothing in this Agreement serves to establish a partnership, joint venture, or general agency relationship between Stripe and you, or with any Financial Partner. If this Agreement expressly establishes an agency relationship between you as principal and Stripe or its Affiliate as agent, the agency conferred, including your rights as principal and Stripe's or its Affiliate's obligations as agent, is limited strictly to the stated appointment and purpose and implies no duty to you, or Stripe or its Affiliate, and will in no event establish an agency relationship for tax purposes.

15.11 Severability.

If any court or Governmental Authority determines a provision of this Agreement is unenforceable, the parties intend that this Agreement be enforced as if the unenforceable provision were not present, and that any partially valid and enforceable provision be enforced to the extent that it is enforceable.

15.12 Cumulative Rights; Injunctions.

The rights and remedies of the parties under this Agreement are cumulative, and each party may exercise any of its rights and enforce any of its remedies under this Agreement, along with all other rights and remedies available to it at law, in equity or under the Financial Services Terms. Any material breach by a party of Section 7 or Section 8 of these General Terms could cause the non-breaching party irreparable harm for which the non-breaching party has no adequate remedies at law. Accordingly, the non-breaching party is entitled to seek specific performance or injunctive relief for the breach.

15.13 Entire Agreement.

This Agreement constitutes the entire agreement and understanding of the parties with respect to the Services, and supersedes all prior and contemporaneous agreements and understandings.

Definitions

"**AAA Rules**" means the American Arbitration Association's Commercial Arbitration Rules as described in Section 13.1(b) of the General Terms.

"**ACH Network**" means the automated clearinghouse payment network that the member organizations of Nacha control and manage.

"**Acquirer Terms**" means the terms that a Payment Method Acquirer has specified that apply to that Payment Method Acquirer's services, located on or accessible from the Stripe Legal Page.

"**Activity**" means any action taken on or related to a Connected Account that a Stripe Connect Platform or a Connected Account initiates, submits or performs, either through the Stripe Technology or through the Stripe Connect Services, including communication regarding the Services as related to that Connected Account.

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by, or is under common Control with another entity.

"**Asset Account**" means the account in which funds are maintained to support the extension of credit in connection with the Stripe Issuing Programs, which is, depending on which Stripe Issuing Program you participate in, your Issuing top-up balance, your Acquiring Receivables balance (as defined in the applicable Issuing Bank Terms), or your Financial Account.

"**Authorized Purpose**" means the purpose approved by Stripe under Section 2.1 of the Stripe Financial Connections Terms for which you may collect, use, disclose and process Connections Data.

"**Available Treasury Balance**" means the amount of funds that is available to be transferred or paid out of a Financial Account.

"**Beta**" means "proof of concept," "beta," "pilot," "invite only" or similar designation.

"**Beta Service**" means any Beta portion of the Services or Stripe Technology.

"**Card**" means a Card Network-branded payment card (which may be a physical card or tokenized, encrypted, or digitized form of a physical card) an Issuing Bank issues to a Stripe Issuing Accountholder for the Stripe Issuing Accountholder's business purposes in connection with the Stripe Issuing Programs.

"**Card Account Data**" means (a) Stripe Data generated by your use of the Stripe Issuing Services; and (b) Personal Data that you (or, if applicable, your Stripe Connect Platform) provide to the applicable Issuing Bank through Stripe for the Stripe Issuing Services, or that you authorize Stripe and any Issuing Bank to collect in relation to the Stripe Issuing Services.

"**Card Authorized User**" means an individual a Stripe Issuing Accountholder authorizes to use a Card to make Card Transactions on the Stripe Issuing Accountholder's behalf (e.g., the Stripe Issuing Accountholder's employee or representative).

"**Card Authorized User Terms**" means the terms governing a Card Authorized User's use of a Card.

"**Card Dispute**" means a dispute in relation to a Card Transaction between you and the merchant or seller of a good or service.

"**Card Network**" means a payment card network, including the network operated by each of Visa, Mastercard, American Express and Discover.

"**Card Network Rules**" means the Payment Method Rules published by a Card Network.

"**Card Transaction**" means a transaction a Stripe Issuing Accountholder or its Card Authorized User initiates to make a payment with a Card or to obtain cash at an automatic teller machine (ATM).

"**CCPA**" means California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199.

"**Change of Control**" means (a) an event in which any third party or group acting together, directly or indirectly, acquires or becomes the beneficial owner of, more than 50% of a party's voting securities or interests; (b) a party's merger with one or more third parties; (c) a party's sale, lease, transfer or other disposal of all or substantially all of its assets; or (d) entering into of any transaction or arrangement that would have the same or similar effect as a transaction referred to in the foregoing (a)-(c); but, does not include an initial public offering or listing.

"**Claim**" means any claim, demand, government investigation or legal proceeding made or brought by a third party.

"**Climate Project**" means a climate project that Stripe funds.

"**Communication**" means any written or electronic transmission of information or communication, including a notice, approval, consent, authorization, agreement, disclosure or instruction.

"**Connected Account**" means (a) a Platform User that has a Stripe account onboarded to a Stripe Connect Platform via the Stripe Connect services; or (b) if the Platform User does not have a Stripe account, then a Platform User to which you have, as a Stripe Connect Platform, sent funds using the Stripe Connect Services.

"**Connected Account Agreement**" means the agreement with Stripe that applies to Connected Accounts (except Payout Recipients), which is accessible on the Stripe Legal Page for the Connected Account's jurisdiction.

"**Connected Account Data**" means data about Connected Accounts and Activity, which may include Protected Data and Stripe Data.

"**Connections Data**" means data associated with a Connections End User's financial account that Stripe provides to you through the Stripe Financial Connections Services, which may include account and routing numbers, account ownership information, account balance, and account transactions, from Data Sources.

"**Connections End User**" means an End User whose Connections Data you request to access, collect, use, and process in connection with the Stripe Financial Connections Services.

"**Content**" means all text, images, and other content that Stripe does not provide to you and that you upload, publish or use in connection with the Services.

"**Control**" means direct or indirect ownership of more than 50% of the voting power or equity in an entity.

"**Credential Compromise**" means an unauthorized access, disclosure or use of your Stripe Account credentials.

"**Custodial Account**" means a custodial account that SPC maintains, in its name, at the Treasury Bank, for the benefit of all accountholders using the Stripe Treasury Services.

"**Custom Account**" means a Connected Account enrolled as a Custom account, as described in the Documentation.

"**Customer**" means an entity or individual who owes payment to you in exchange for you providing goods or services (including charitable services).

"**Cut-Off Time**" means the time on a business day by which SPC must receive an instruction or Financial Account Transaction request from a Stripe Treasury Accountholder in order to process that instruction or request on the same day.

"**Data Source**" means an entity that provides financial account information to Stripe.

"**Data Processing Agreement**" means the data processing agreement located at www.stripe.com/[countrycode]/legal/dpa, where "[countrycode]" means the two-letter abbreviation for the country where your Stripe Account is located.

"**Data Warehouse**" means a data storage solution listed on the Stripe Website that you select.

"**Dispute**" means an instruction a Customer initiates to reverse or invalidate a processed Transaction (including "chargebacks" and "disputes" as those terms may be used by Payment Method Providers).

"**Documentation**" means the sample code, instructions, requirements and other documentation (a) available on the Stripe Website, the first page of which is located at **www.stripe.com/docs**; and (b) included in the Stripe SDKs.

"**Due Diligence Requirements**" means requirements imposed by Law that govern, are related to, or are similar to Anti-Money Laundering (AML), Know Your Customer (KYC), Know Your Business (KYB) and Customer Due Diligence (CDD).

"**End User**" has the meaning given in Stripe's **Privacy Policy**.

"**End User Rights**" means the data privacy rights afforded to End Users under Law, including the CCPA and GDPR.

"**End User Service**" has the meaning given in the **Stripe End User Terms**.

"**Entry**" has the meaning given to it in the Nacha Operating Rules.

"**ERISA**" means the Employee Retirement Income Security Act of 1974, 29 U.S.C. Chapt. 18.

"**Express Account**" means a Connected Account enrolled as an Express account, as described in the Documentation.

"**Express Consent**" means a Connections End User's express, informed opt-in consent to your collection, use, disclosure, and processing of that Connections End User's Connections Data for the Authorized Purpose.

"**Express Consent UI**" means the user interface, including the text and consent mechanism included on that user interface, through which you obtain Express Consents.

"**FCRA**" means Fair Credit Reporting Act, 15 U.S.C. Section 1681, et seq. and Equal Credit Opportunity Act, 15 U.S.C. Section 1681, et seq.

"**FDIC**" means Federal Deposit Insurance Corporation.

"**FDIC Insurance**" means deposit insurance that covers certain types of accounts at FDIC-insured banks.

"**Feedback**" means ideas, suggestions, comments, observations and other input you provide to Stripe regarding Stripe services and the Stripe Technology.

"**Fees**" means the fees applicable to the Services.

"**Financial Account**" means the virtual prepaid access account that SPC or its Affiliates creates for a Stripe Treasury Accountholder as part of the Stripe Treasury Services.

"**Financial Account Transaction**" means an Entry or other transaction in a Financial Account that adds to or subtracts from the Available Treasury Balance.

"**Financial Institution**" has the meaning given in the GLBA.

"**Financial Partner**" means a third party or an Affiliate of Stripe that provides financial services and with which Stripe or its Affiliate interacts to provide the Services.

"**Financial Services Terms**" means (a) the rules and terms a Financial Partner specifies that apply to that entity's services; and (b) the PCI Standards.

"**Force Majeure Event**" means an event beyond the control of Stripe or its Affiliates, including a strike or other labor dispute; labor shortage, stoppage or slowdown; supply chain disruption; embargo or blockade; telecommunication breakdown; power outage or shortage; inadequate transportation service; inability or delay in obtaining adequate supplies; weather; earthquake; fire; flood; act of God; riot; civil disorder; civil or government calamity; epidemic; pandemic; state or national health crisis; war; invasion; hostility (whether war is declared or not); terrorism threat or act; Law; or act of a Governmental Authority.

"**GLBA**" means Gramm-Leach Bliley Act, 15 U.S.C. Sections 6802-6809.

"**Governmental Authority**" means a regulator or other governmental agency or entity with jurisdiction over the Services, Stripe or you, as applicable.

"**High-Risk Jurisdiction**" means any jurisdiction or administrative region that Stripe has deemed to be of particularly high risk, as identified on the **Stripe Restricted Business List**.

"**High-Risk Person**" means any individual or entity that Stripe has deemed to be of particularly high risk, as identified on the **Stripe Restricted Business List**.

"**Hold**" means a restriction on the availability of funds in a Financial Account that Stripe or its Affiliate places as a result of delayed funds availability, Legal Process or other reason.

"**ID Image**" means an image of an individual submitted through the Stripe Identity Services, including an image captured from an individual's identification document.

"**Insolvency Proceeding**" means the occurrence of any of the following (or any analogous procedure or step):

(a) as defined by Law, you are unable (or deemed to be unable) to pay your debts;

(b) you are the subject of a petition, resolution, order or any other step in relation to winding up, bankruptcy or equivalent proceedings;

(c) you stop, or threaten to stop, carrying on all or part of your business (except for the purposes of an amalgamation, reconstruction or reorganization);

(d) you enter into a compulsory or voluntary liquidation, or a liquidator is appointed in relation to you or any of your assets;

(e) you are the subject of a petition for an administration order or an application for such an order, or a notice of intention to appoint an administrator to you is given, or any other step is taken by any individual or entity with a view to the administration of you under Law;

(f) a moratorium is agreed or declared with respect to all or part of your debts;

(g) you enter, or propose to enter, into any compromise or arrangement of your debts with or for the benefit of some or all of your creditors generally, or in respect of a particular type of your debts;

(h) you begin proceedings or negotiations, or propose or agree, to reschedule, readjust or defer your debts;

(i) a liquidator, receiver, administrative receiver, administrator, manager or other similar officer is appointed in respect of the whole or any part of your assets;

(j) an enforcement of any security over, or an execution, attachment, lien, levy, distress or similar procedure is levied against, any of your assets;

(k) any legal proceeding, corporate action or other procedure or step is taken in connection with appointing an administrator, administrative receiver, receiver, liquidator, manager, trustee in bankruptcy or other similar officer in relation to you or any of your assets; or

(l) where any User Group Entity or shareholder of a User Group Entity is subject to any of the events listed in this definition.

"**IP Claim**" means a Claim made against you by a third party alleging that the Stripe Technology, Services or a Stripe Mark provided to and used by you in accordance with this Agreement infringes or misappropriates the IP Rights of the third party making the Claim, excluding Claims made by Connected Accounts.

"**IP Claim Losses**" means (a) all amounts finally awarded to the third party making an IP Claim; and (b) all amounts paid to a third party to settle an IP Claim under an agreement approved by Stripe.

"**IP Rights**" means all copyrights, patents, trademarks, service marks, trade secrets, moral rights and other intellectual property rights.

"**IRS**" means Internal Revenue Service.

"**IRS Code**" means Internal Revenue Code, 26 U.S.C. Title 26.

"**Issuing Bank**" means the Financial Partner, identified in the Issuing Bank Terms for the applicable Stripe Issuing Program, that issues a Card.

"**Issuing Bank Terms**" means the applicable Issuing Bank's Financial Services Terms that govern your participation in the applicable Stripe Issuing Program.

"**Issuing Complaint**" means any expression of dissatisfaction with a product, service, policy, or employee related to a Stripe Issuing Program.

"**Law**" means all applicable laws, rules, regulations and other binding requirements of any Governmental Authority.

"**Legal Process**" means a writ of attachment, lien, levy, subpoena, warrant, or other legal order.

"**Mark**" means a trademark, service mark, design mark, logo or stylized script.

"**Multi-Currency Processing**" means the ability to have funds settled to a User Bank Account in a currency different from the one in which you accepted payment from a Customer.

"**Nacha**" means the National Automated Clearinghouse Association.

"**Nacha Operating Rules**" means the rules Nacha publishes that govern automated clearing house transactions on the ACH Network, located at **www.nachaoperatingrulesonline.org**.

"**Originator**" has the meaning given to it in the Nacha Operating Rules.

"**Payment Account Details**" means the Payment Method account details for a Customer that the PCI Standards require to be protected, which may include the Customer's name, and with respect to credit and debit cards, the Customer's account number, card expiration date, and card verification value or similar security code.

"**Payment Method**" means a payment method that Stripe accepts as part of the Stripe Payments Services (e.g., a Visa credit card, Klarna).

"**Payment Method Acquirer**" means an entity that a Payment Method Provider has authorized to (a) sponsor or submit Transactions at the request of merchants to the Payment Method Provider for authorization and clearing; and (b) receive and remit settlement funds for authorized and cleared Transactions.

"**Payment Method Provider**" means the provider of a Payment Method (e.g., Visa Inc., Klarna Bank AB).

"**Payment Method Rules**" means the guidelines, bylaws, rules and regulations a Payment Method Provider imposes that describe how a Payment Method may be accepted and used.

"**Payment Method Terms**" means terms that apply to your acceptance and use of a Payment Method, located on or accessible from the Stripe Website, including on the Stripe Legal Page, and which as of the Effective Date are described on that page as "Payment Method Terms."

"**Payout Delay**" means a delay to the Payout Schedule caused by (a) the unavailability of a Financial Partner, Governmental Authority, telecommunications provider or internet service provider; (b) incorrect information, such as a bank account number, provided to Stripe; (c) your equipment, software, or other technology; or (d) a Force Majeure Event.

"**Payout Recipient**" means a third-party recipient to which Stripe enables you to make payouts via the Stripe Connect Services.

"**Payout Schedule**" means the schedule available in the Stripe Dashboard that shows the number of business days following the Transaction date that it takes for Stripe to initiate transfer of Transaction settlement funds to a User Bank Account.

"**PCI-DSS**" means the Payment Card Industry Data Security Standards.

"**PCI Standards**" means PCI-DSS and Payment Application Data Security Standard (PA-DSS), including successor standards (if any).

"**Personal Data**" means any information relating to an identifiable natural person that is Processed (as defined in the **Data Processing Agreement**) in connection with the Services, and includes "personal data" as defined under EU Regulation (EU) 2016/679 (General Data Protection Regulation) and "personal information" as defined under the CCPA.

"**Platform Provider Agreement**" means, collectively, the agreements that a Stripe Connect Platform has with its Connected Accounts.

"**Platform Services**" means the products and services that Platform Users receive from a Stripe Connect Platform, regardless of whether fees are charged (e.g., web development, customer support or hosting services).

"**Platform User**" means, where you are acting as a Stripe Connect Platform, a user of your platform.

"**Pooled Account**" means a pooled account to which Transaction settlement funds are credited.

"**Principal Owner**" means, with respect to a legal entity, an individual who directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise, owns at least 25% of the equity interests of the legal entity.

"**Privacy Policy**" means any or all of a publicly posted privacy policy, privacy notice, data policy, cookies policy, cookies notice or other similar public policy or public notice that addresses a party's Personal Data practices and commitments.

"**Protected Data**" means (a) all User Information that you provide to Stripe; and (b) any Personal Data that Stripe uses when acting as a "Data Processor" (as defined in the Data Processing Agreement) when providing the Services.

"**Radar Score**" means a numerical risk score or level associated with a Transaction or other related activity that the Stripe Radar Services provides.

"**Refund**" means an instruction you initiate to provide a full or partial return of funds to a Customer for a processed Transaction.

"**Representative**" means an individual submitting your application for a Stripe Account.

"**Reserve**" means funds described as such by Stripe, which Stripe holds as security against liabilities you incur under this Agreement.

"**Restricted Business**" means any category of business or business practice for which a Service cannot be used, as identified on the Stripe Restricted Business List (located on the Stripe Website) for the applicable Service and jurisdiction of your Stripe Account.

"**Reversal**" means the reversal of the settlement of funds for a Transaction.

"**Selfie Verification**" means the verification of an ID Image using biometric identifiers and facial recognition technology.

"**Service**" means a service Stripe (or its Affiliate, as applicable) makes available to you under this Agreement.

"**Services Terms**" means terms in this Agreement that apply to particular Stripe services (e.g., Stripe Payments Terms).

"**SDP Data**" means data you transfer from your Stripe Account to a Data Warehouse.

"**SPC**" means Stripe Payments Company, which is a Stripe Affiliate.

"**Standard Account**" means a Connected Account enrolled as a Standard account, as described in the Documentation.

"**Stripe Account**" means your Stripe account.

"**Stripe API**" means all instances of the Stripe application programming interfaces, including all endpoints that enable Stripe users to use Stripe services.

"**Stripe Climate**" means a suite of features Stripe provides that are designed to enable you to create and run your own corporate climate program.

"**Stripe Climate Funds**" means the amount you choose to voluntarily allocate to Climate Projects through Stripe Climate, as a percentage of your revenue or a flat monthly amount, or another method of calculation Stripe accepts.

"**Stripe Connect Platform**" means a platform provider that uses the Stripe Connect Services.

"**Stripe Connect Services**" means (a) if you are a Stripe Connect Platform, the Services that enable you to create and manage Stripe accounts connected to your platform, as described in the Documentation; or (b) if you are a Connected Account, the Services described in the Connected Account Agreement.

"**Stripe Dashboard**" means the interactive user interface through which a Stripe user may view information about and manage a Stripe account.

"**Stripe Data**" means data that you obtain via the Services, including (a) information relating to Stripe API interactions via the Stripe Technology; (b) information Stripe uses for security or fraud prevention; and (c) all aggregated information Stripe generates from the Services.

"**Stripe Data Pipeline Services**" means the Services that enable you to send data from your Stripe Account to your Data Warehouse account, as described on the Stripe Website.

"**Stripe End User Terms**" means the terms that apply to an End User's use of Stripe's End User Services located at **www.stripe.com/legal/end-users**.

"**Stripe Financial Connections Services**" means the Services that enable you to verify End User financial accounts and the option to receive Connections Data.

"**Stripe Identity Services**" means the Services that enable Stripe to collect and verify, and Stripe and you to store, information regarding individuals for the purpose of verifying the identity of those individuals.

"**Stripe Identity Services Documentation**" means the Documentation, along with other documentation that Stripe makes available to you (including via email and the Stripe Dashboard), relating to the Stripe Identity Services.

"**Stripe Issuing Account**" means the account an Issuing Bank maintains for a Stripe Issuing Accountholder, and each subaccount to that account.

"**Stripe Issuing Accountholder**" means a business or organization that has successfully completed the onboarding requirements described in the Stripe Issuing Accountholder Terms and been approved for a Stripe Issuing Account.

"**Stripe Issuing Administrator**" means the individual that a Stripe Issuing Accountholder appoints to manage its participation in the Stripe Issuing Programs.

"**Stripe Issuing Platform Services**" means the Services that allow you to co-market the Stripe Issuing Services to your Platform Users and provide access to the Stripe Issuing Services to Accountholders.

"**Stripe Issuing Program**" means Card issuing services that the applicable Issuing Bank provides under the applicable Issuing Bank Terms, together with the Stripe Issuing Services.

"**Stripe Issuing Program Guidelines**" means all product design, marketing, compliance, reporting, and other guidelines and requirements Stripe and the applicable Issuing Banks establish related to the Stripe Issuing Services, as updated from time to time.

"**Stripe Issuing Program Territory**" means the Territory, as that term is defined in the applicable Issuing Bank Terms.

"**Stripe Issuing Services**" means Services that Stripe and its Affiliates make available to Stripe Issuing Accountholders, on behalf of Issuing Banks, and related Stripe services, including (a) integration with Issuing Banks; (b) providing Stripe Issuing Accountholders with access to Cards; (c) enabling Stripe Issuing Accountholders to manage Card spend, and (d) other services described in the Stripe Issuing Accountholder Terms.

"**Stripe Legal Page**" means www.stripe.com/[countrycode]/legal, where "[countrycode]" means the two-letter abbreviation for the country where a Stripe Account is located.

"**Stripe Losses**" means all amounts awarded to the third party making a Claim, and all penalties, fines, and third-party costs (including legal fees) paid by the Stripe Parties.

"**Stripe Parties**" means Stripe, Stripe's Affiliates, and the directors, employees and agents of each.

"**Stripe Payments Services**" means the Services that enable you to accept and refund Customer payments, perform related financial transactions, and manage Customer disputes.

"**Stripe Pricing Page**" means www.stripe.com/[countrycode]/pricing, where "[countrycode]" means the two-letter abbreviation for the country where a Stripe Account is located.

"**Stripe Radar Data**" means the Radar Scores and other data you receive through the Stripe Radar Services.

"**Stripe Radar Services**" means the Services that are designed to enable you to detect and evaluate the risk that a Transaction or other related activity is fraudulent.

"**Stripe SDK**" means a software development kit listed on **www.github.com/stripe**.

"**Stripe Tax Data**" means data and reporting you receive through the Stripe Tax Services.

"**Stripe Tax Services**" means the Services that are designed to enable you to determine and calculate the amount, if any, of certain Taxes due in connection with your sale of goods or provision of services to Customers.

"**Stripe Technology**" means all hardware, software (including software in the Stripe SDKs), application programming interfaces (including the Stripe API), user interfaces (including the Stripe Dashboard), and other technology that Stripe uses to provide and make available the Stripe services.

"**Stripe Terminal Documentation**" means the Documentation, along with other documentation that Stripe makes available to you (including via email), relating to the Stripe Terminal Services, Stripe Terminal Software or Stripe Terminal Products.

"**Stripe Terminal Product**" means a device, instrument, piece of equipment or other hardware that (a) Stripe, its Affiliate, or a third-party distributor or reseller authorized by Stripe or its Affiliate supplies to you, which may be a physical Point of Sale (POS) device, accessory, component, or spare part, and the Terminal Device Software installed on that hardware product; or (b) Stripe approves for use to access the Stripe Terminal Services or the Stripe Technology, or to operate the Stripe Terminal Software.

"**Stripe Terminal Services**" means the Stripe Payments Services for Transactions processed using a Stripe Terminal Product, together with related services and features as described in the Stripe Terminal Documentation and on the Stripe Website.

"**Stripe Terminal Software**" means the Terminal Device Software and Terminal SDK.

"**Stripe Treasury Accountholder**" means a Connected Account, or Stripe Connect Platform using the Stripe Treasury Services for your own business purpose, who has successfully completed the onboarding requirements described in the Stripe Treasury Platform Terms.

"**Stripe Treasury Account Information**" means Personal Data or business information that a Stripe Connect Platform provides on behalf of its Connected Accounts to enable Stripe and its Affiliates to (a) determine the Connected Accounts' eligibility to access the Stripe Treasury Services; (b) make the Stripe Treasury Services available to Stripe Treasury Accountholders; and (c) fulfill their responsibilities to applicable Treasury Banks and Treasury Transfer Networks.

"**Stripe Treasury Dashboard**" means a user interface a Stripe Connect Platform provides that enables a Stripe Treasury Accountholder to manage its Financial Account.

"**Stripe Treasury Product Guidelines**" means all product design, marketing, compliance, reporting and other guidelines and requirements established by Stripe, its Affiliates or the applicable Treasury Banks from time to time in connection with the Stripe Treasury Services.

"**Stripe Treasury Services**" means the Services that enable a Stripe Treasury Accountholder to create and maintain a Financial Account where the Stripe Treasury Accountholder can (a) store, spend, and manage funds; and (b) make electronic payments and funds transfers to and from that account.

"**Stripe Treasury Territory**" means the United States and Puerto Rico.

"**Stripe Website**" means **www.stripe.com**.

"**Tax**" or "**Taxes**" means any applicable taxes and duties imposed by any Governmental Authority, including sales and use tax, excise tax, gross receipts tax, value-added tax (VAT), goods and services tax (GST) (or equivalent transaction taxes) and withholding tax.

"**Tax Information Report**" means a required tax information return or report, including IRS Form 1099, IRS Form 1042-S, or any other similar form.

"**Terminal Device EULA**" means the Terminal Device Software License Agreement for end users, the terms of which are incorporated into this Agreement by this reference.

"**Terminal Device Software**" has the meaning given to it in the Terminal Device EULA.

"**Terminal Purchase Terms**" means the agreement under which Stripe or its Affiliate supplies the Stripe Terminal Products that you are using.

"**Terminal SDK**" means the software code that is Stripe Technology and is distributed under the MIT license, test environment, and associated documentation, as described in the Stripe Terminal Documentation and which Stripe makes available at **https://github.com/stripe**, including iOS, Android and JavaScript versions, and including all Updates.

"**Third-Party Service**" means a service, product, or promotion provided by a third party that utilizes, integrates with or is ancillary to the Services.

"**Transaction**" means a Payment Method transaction request initiated via the Stripe Technology through which Stripe is directed to capture funds for or from a payer's associated account with respect to a payment from a Customer to you, and includes the authorization, settlement and if applicable, Disputes, Refunds and Reversals with respect to that Payment Method transaction request.

"**Treasury Authorized User**" means an individual that a Stripe Treasury Accountholder authorizes to use the Stripe Treasury Services.

"**Treasury Bank**" means a bank insured by the Federal Deposit Insurance Corporation through which Stripe or its Affiliate holds Stripe Treasury Accountholder funds.

"**Treasury Regulatory Requirements**" means Law, the rules of the Treasury Transfer Networks and the PCI Standards.

"**Treasury Transfer Networks**" means the electronic funds transfer networks the Stripe Treasury Services uses, including the ACH Network, credit card networks, and debit card networks.

"**Update**" means a modification, feature enhancement or update to the Services or Stripe Technology that requires you to take some action, which may include changing your implementation of the Services or Stripe Technology.

"**User Affiliate Reserve**" means funds described as a reserve by Stripe, which Stripe or its Affiliate holds as security against liabilities that any User Group Entity incurs under its agreement with Stripe or an Affiliate of Stripe.

"**User Bank Account**" means a bank or other financial institution account you identify to Stripe.

"**User Compliance Information**" means information about you that Stripe requires to comply with Law, and Governmental Authority and Financial Partner requirements, and may include information (including Personal Data) about your representatives, beneficial owners, principals and other individuals associated with you or your Stripe Account.

"**User Financial Information**" means (a) information about you that Stripe requires to assess your business and financial condition and outstanding credit exposure, including financial statements (and, where applicable, unaudited management accounts including a profit and loss account, balance sheet and cash-flow statement) and supporting documentation (including bank statements); (b) information and supporting documentation to enable Stripe to calculate your risk of loss; and (c) all other information Stripe requests to assess your risk and ability to perform your obligations under this Agreement.

"**User Group**" means (a) you; (b) any entity or individual that Stripe reasonably determines is associated with you; and (c) each of your and their Affiliates; that has entered into an agreement with Stripe (or an Affiliate of Stripe) under which Stripe or its Affiliate provides services.

"**User Group Entity**" means an individual or entity that is part of the User Group (including you).

"**User Information**" means User Compliance Information and User Financial Information.

"**User Materials**" means any materials that you or a Stripe Issuing Accountholder wish to place on Cards or other materials related to the Stripe Issuing Programs, including any Mark or material protected by any IP Rights.

"**User Party**" means you, your Affiliate, or a director, employee or agent of you or your Affiliate.

"**Verifiable Individual**" means an individual whose Verification Data is submitted through the Stripe Identity Services.

"**Verification Data**" means all data, information, photos, ID Images, and documents (including copies of documents) submitted through the Stripe Identity Services.

Services Terms

- Stripe Payments
- Stripe Connect - Platform
- Stripe Automatic Currency Conversion
- Stripe Climate
- Stripe Data Pipeline
- Stripe Financial Connections
- Stripe Identity
- Stripe Issuing - Accountholder
- Stripe Issuing - Platform
- Stripe Radar
- Stripe Tax
- Stripe Terminal
- Stripe Terminal - Platform
- Stripe Treasury - Connected Accounts
- Stripe Treasury - Platform

Stripe Services Agreement
Stripe Connected Account Agreement
Stripe Payments Company Terms

stripe

Stripe Payments Company Terms

Last updated: August 22, 2022

These Stripe Payments Company Terms ("**SPC Terms**") form a legal agreement between Stripe Payments Company ("**SPC**") and the entity or sole proprietor on whose behalf a Stripe account is created ("**you**" and "**your**"). SPC is a U.S. state-licensed money transmitter and federally registered money services business. These SPC Terms are effective upon the date you first access or use the SPC Services and continue until these SPC Terms terminate.

Certain Services may involve regulated money transmission under U.S. Law. To the extent your use of the Services involves money transmission or other regulated services under U.S. Law, those services are the "**SPC Services**" and are provided to you by SPC, not by Stripe or any other Stripe Affiliate, unless applicable Services Terms specify otherwise. These SPC Terms state the terms and conditions that apply to your use of the SPC Services.

1. Relationship to Stripe Services Agreement.

In addition to these SPC Terms, you must also have a Stripe Services Agreement in place with Stripe for technology services that enable instructions to be relayed to SPC. SPC will not charge you fees for the provision of the SPC Services; fees payable for the Services (including technology services related to the SPC Services) will be determined under the Stripe Services Agreement.

1.1 Terms that Apply to You.

You expressly agree to the terms and conditions of these SPC Terms, the Stripe Services Agreement, and any updates or modifications to either of those documents made from time to time by SPC or Stripe. Undefined capitalized terms used in these SPC Terms have the meanings given to them in the Stripe Services Agreement. You represent as of the Effective Date, and warrant at all times during the Term, that all of the information that you provide to SPC directly or through your use of the Services is accurate and complete, and that you are authorized to agree to these SPC Terms.

1.2 Incorporation of Stripe Services Agreement.

These SPC Terms are Financial Services Terms under the Stripe Services Agreement. These SPC Terms incorporate by this reference the terms of the Stripe Services Agreement, including the terms incorporated within the Stripe Services Agreement; except, for purposes of the SPC Services, each reference to "Stripe" in the Stripe Services Agreement will be read as a reference to SPC, each reference to "Agreement" in the Stripe Services Agreement will be read to include these SPC Terms, and the incorporated terms will be limited to the SPC Services. All other parts of the Services will remain governed by the Stripe Services Agreement between you and Stripe.

1.3 Inconsistency.

To the extent there is a conflict between the Stripe Services Agreement and these SPC Terms, these SPC Terms will prevail with respect to the SPC Services. In addition, to the extent there is a conflict between applicable Services Terms and these SPC Terms with respect to the SPC Services, the applicable Services Terms will prevail.

2. The SPC Services.

2.1 Ability to Instruct SPC.

By using the Stripe API or your Stripe Dashboard, you may use the Services to send instructions to SPC to add funds to and redeem funds from accounts that you maintain with SPC and to transfer funds to third parties or to yourself.

2.2 Adding funds.

(a) *Methods of Adding Funds*. You may add funds to accounts you maintain with SPC from User Bank Accounts or accounts you maintain with SPC or its Affiliate through one or more methods. Depending on the Services available to you, these methods may include bank transfers, payment cards, transfers from other accounts you maintain with Stripe or its Affiliate, or other methods we may make available. You may pass information to SPC and its Affiliates for purposes of adding funds to accounts that you maintain with SPC, including bank account information, payment card numbers, cardholder names, or other applicable information. When you provide this information, you represent as of the date you provide it, and warrant at all times during the Term, that the information is correct and that you are authorized to access and transmit those funds. You authorize SPC and its Affiliates to use this information to initiate debits to your User Bank Accounts or accounts you maintain with SPC or its Affiliate.

(b) *Debit Authorizations*. With respect to bank transfers, you authorize SPC and its Affiliates to debit each User Bank Account without separate notice, and according to the applicable **User Bank Account Debit Authorization**, to add or transfer funds to accounts you maintain with SPC. SPC and its Affiliates may rely on this authorization to make one or more debits to add or transfer funds. This debit authorization will remain in full force and effect until all of the accounts you maintain with SPC are closed. If applicable debit scheme authorization rules grant you the right to revoke your debit authorization, then to the extent Law permits, you waive that right.

2.3 Transferring or redeeming funds.

You may instruct SPC to redeem funds from accounts you maintain with SPC and to transfer funds to third parties or to yourself. Depending on the Services available to you, you may transfer or redeem funds from User Bank Accounts or accounts you maintain with SPC or its Affiliate. You may provide transfer or redemption instructions to SPC and its Affiliates, including information to identify your intended recipient, the date on which you would like your transfer or redemption to occur, and the currency amount of the transfer or redemption. SPC will use this information to attempt to complete the requested transfer or redemption.

2.4 SPC's obligation to transfer or redeem funds.

SPC will attempt to transfer or redeem funds as you instruct. SPC will return to you any funds that cannot be transferred or redeemed per your instructions, subject to the following conditions. Depending on the information you provide, and your other use of the SPC Services and the Services, you agree to allow SPC to pause or terminate any transfers or redemptions for illegal activity, fraud, risk or compliance purposes, which may include (a) withholding funds to offset chargeback or other fraud losses owed to SPC or its Affiliate; (b) interdicting funds for legal or compliance purposes, such as to comply with U.S. sanctions obligations; and (c) suspending your use of the SPC Services.

2.5 Pooled Accounts.

SPC will hold all funds it receives from you for the purpose of adding funds to accounts you maintain with SPC or transferring funds to third parties or to yourself, together with funds SPC holds for other users and will credit your funds to pooled accounts at one or more Financial Partners. SPC will hold your funds for your benefit, and neither SPC nor Stripe will voluntarily make those funds available to creditors in the event of bankruptcy. Depending on where your business is headquartered, additional protections may apply to the funds under your state's money transmission laws.

2.6 Investment of Funds.

To the extent Law, the applicable Financial Services Terms and applicable Services Terms permit: (a) SPC may invest the funds that it holds in pooled accounts into liquid investments; (b) SPC owns the earnings from these investments; and (c) you irrevocably assign to SPC all rights you have (if any) to earnings from these investments.

2.7 Your use of SPC Services.

You may not use the SPC Services for illegal activities or for any of the business activities found on the **Restricted Business List**.

2.8 SPC privacy practices.

SPC will receive data when you use the SPC Services. SPC will treat your data and protect your privacy according to Stripe's **Privacy Policy**.

3. SPC Services not available for personal, family, or household use.

You may not use the SPC Services for personal, family, or household use, unless applicable Services Terms specify otherwise. By using the SPC Services, you represent as of the Effective Date and warrant at all times during the Term that you are a legal entity or a sole proprietor.

4. Allocation of liability and dispute resolution.

Without limiting the general incorporation of the Stripe Services Agreement, please ensure that you carefully review the following provisions:

(a) Sections 5, 10, 11 and 12 of the General Terms, which allocate responsibility and liability between you and SPC with respect to matters arising under these SPC Terms; and

(b) Section 13 of the General Terms, which provides that a dispute, claim or controversy arising out of or relating to statutory or common law claims, the breach, termination, enforcement, interpretation or validity of any provision of these SPC Terms, and the determination of the scope or applicability of your agreement to arbitrate any dispute, claim or controversy originating from these SPC Terms, but specifically excluding any dispute principally related to either party's IP Rights (which will be resolved in litigation before the United States District Court for the Northern District of California), will be determined by arbitration in San Francisco, California before a single arbitrator.

5. Termination.

These SPC Terms automatically terminate if the Stripe Services Agreement terminates for any reason.

6. Contact and complaints.

You can contact SPC at **https://stripe.com/contact** or by mail to Stripe Payments Company, 354 Oyster Point Boulevard, South San Francisco, California, 94080. SPC may provide you with information and notifications in relation to the SPC Services via your Stripe Dashboard.

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

- Cross River Bank
- PNC Bank
- Wells Fargo Bank

Issuing Bank Terms

Payment Method Terms

User Bank Debit Authorizations

Restricted Businesses

Other Products and Programs

- Stripe Terminal Device EULA
- Stripe Terminal Purchase Terms
- Stripe Terminal Reseller Terms
- Stripe Atlas Agreement
- Stripe Climate Contribution Terms

Stripe Apps

- App Developer Agreement
- App Marketplace Agreement

Privacy

- Privacy Policy
- Cookies Policy
- Privacy Shield Policy
- Service Providers List
- Data Processing Agreement
- Stripe Privacy Center

Intellectual Property

- Intellectual Property Notice
- Marks Usage

E-SIGN Disclosure

Licenses

stripe

United States

English (United States)

Products

Atlas
Billing
Capital
Checkout
Climate
Connect
Corporate Card
Data Pipeline
Elements
Financial Connections
Identity
Invoicing
Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Solutions

Enterprises
SaaS
Marketplaces
Creator Economy
Finance Automation
Platforms
Ecommerce
Crypto
Embedded Finance
Global Businesses

Integrations & Custom Solutions

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Resources

Support Center
Support Plans
Guides
Customer Stories
Blog
Annual Conference
Contact Sales
Privacy & Terms
Licenses
COVID-19
Sitemap
Cookie Settings
Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

Payment Method Terms

Last updated: 2023-03-31

On this page

Last Updated: June 5, 2023

Payment Method Terms are terms that apply to the use of Payment Methods. You can decide whether or not to use a Payment Method. However, if you use a Payment Method, you accept and agree to the terms applicable to that Payment Method, which will form part of your agreement with Stripe.

Payment Methods

- ACH
- ACCS/PAD
- Affirm
- Afterpay / Clearpay
- Alipay
- American Express (Switzerland)
- Amex Express Checkout
- Apple Pay on the Web
- Bancontact
- BECS Direct Debit (Australia)
- Cartes Bancaires
- Cash App
- eftpos

- EPS
- FPX
- giropay
- Google Pay
- GrabPay
- iDEAL
- Interac
- Konbini
- Link
- Masterpass
- Multibanco
- PayNow
- SEPA Direct Debit
- SOFORT
- US Debit Cards
- Visa Checkout
- WeChat

The above list is not an exhaustive list of the Payment Methods offered by Stripe, and there are Payment Methods for which there are no separate Payment Method Terms.

Payment Method availability also varies by geography. Depending on your location, you may not be able to use one or more of the Payment Methods listed above (or that are otherwise offered by Stripe). The Payment Methods available to you are set out in your Stripe dashboard.

Amendments and changes

Payment Methods are sourced from various providers, and each provider controls the terms that apply to its Payment Method. As a consequence, the terms and **Documentation** applicable to a Payment Method are subject to change at any time, and it is your responsibility to periodically review the terms and Documentation in order to ensure that you are aware of, and comply with, the applicable requirements.

Stripe may add or remove Payment Methods at any time. If Stripe removes a Payment Method, Stripe will provide you with notice prior to the removal becoming effective for you, except where Stripe is required by a third party (such as the Payment Method provider) to cease offering the payment method.

Redirection to online banking pages

Some Payment Methods require the re-direction of the Customer to an online banking page ("Online Banking Payment Methods"). If you use an Online Banking Payment Method, you must ensure that the Customer is able to recognize that the re-direction has occurred via the display of the bank's URL in the address line of the browser, and the Customer must be able to review the security certificate for the bank's online banking page. In addition, you may not use any iframes (or any other method that integrates the online banking page within your site content) when including an Online Banking Payment Method in your payment process.

stripe

User Bank Account Debit Authorizations

By using Stripe services, you agree to Stripe and its affiliates' right to debit your User Bank Account and you authorize Stripe and its affiliates to debit your User Bank Account to collect any fees owed or other amounts due to Stripe or its affiliates or to credit or transfer funds to any of your accounts maintained with Stripe or its affiliates. Your authorization to Stripe and its affiliates extends to any bank account that you link to Stripe services (i.e. any User Bank Account). Your authorization is in complete compliance with any applicable bank debit rules, including the debit scheme authorization and mandate language included below. Your authorization to debit any of your User Bank Accounts includes the specific mandate or authorization language for the specific debit scheme that covers your bank account (e.g. for US bank accounts the ACH/Nacha language will apply and for GB bank accounts the Bacs language will apply). The debit scheme language for each bank scheme is incorporated into your authorization to Stripe and Stripe's affiliates to debit any of your User Bank Accounts with the same force and effect as if you had signed a paper and obtained a hard copy containing the same terms.

US Bank Accounts (ACH/Nacha)

ACH Nacha Authorization

I authorize Stripe and Stripe's Affiliates to periodically debit any of the US User Bank Accounts for any amount owed to Stripe or Stripe's Affiliates under the Stripe Services Agreement or to credit or transfer funds to any of my accounts maintained with Stripe or Stripe's Affiliates, until this authorization is revoked. I waive any prior notice requirements for Stripe and/or Stripe Affiliates to provide me or my company with notice of a debit for amounts owed to Stripe or Stripe's Affiliates or amounts used to credit or transfer funds to any of my accounts with Stripe or Stripe's Affiliates. I confirm that I am the only person required to authorize debits from the User Bank Accounts. I understand that Stripe and Stripe Affiliates will only debit the User Bank Account in accordance with the Stripe Services Agreement or as otherwise agreed between Stripe or Stripe's Affiliates and me. I may amend or cancel this authorization at any time by providing Stripe with 30 days' notice.

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

- Cross River Bank
- PNC Bank
- Wells Fargo Bank

stripe

Prohibited and Restricted Businesses

On this page

Last updated: May 2023

Use of Stripe's services for any dealings, engagement, or sale of goods/services linked directly or indirectly with jurisdictions Stripe has deemed high risk, such as Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk Regions, or persons Stripe has deemed high risk, such as those individuals or entities named to a restricted person or party list of the U.S., United Kingdom, European Union or United Nations, including the sanctions lists maintained by the U.S. Office of Foreign Assets Control or the Denied Persons List or Entity List maintained by the U.S. Department of Commerce, is prohibited. Additionally, it is prohibited to use Stripe's products and services to directly or indirectly export, reexport, sell, or supply accounting, trust and corporate formation, management consulting services, architecture services or engineering services to any person located in Russia. Further, it is prohibited to use Stripe's products and services directly or indirectly related to any goods prohibited by law (e.g. luxury goods) from Russia.

Prohibited Businesses

You must not use Stripe's services for the following activities.

Illegal products and services

- Illegal drugs, substances designed to mimic illegal drugs, and equipment designed for making or using drugs
- Fake references or ID-providing services
- Telecommunications manipulation equipment including jamming devices
- Any business or organization that a. engages in, encourages, promotes or celebrates unlawful violence or physical harm to persons or property, or b. engages in, encourages, promotes or celebrates unlawful violence toward any group based on race, religion, disability, gender, sexual orientation, national origin, or any other immutable characteristic
- Any other products or services that are in violation of law in the jurisdictions where your business is located or targeted to

Products and services that infringe intellectual property rights

Sales or distribution of music, movies, software, or any other licensed materials without appropriate authorization

Counterfeit goods; illegally imported or exported products

Unauthorized sale of brand name or designer products or services

Any other products or services that directly infringe or facilitate infringement upon the trademark, patent, copyright, trade secrets, proprietary or privacy rights of any third party

Products and services that are unfair, predatory, or deceptive

Pyramid schemes

'Get rich quick' schemes including: investment opportunities or other services that promise high rewards to mislead consumers; schemes that claim to offer high rewards for very little effort or up front work; sites that promise fast and easy money; businesses that make outrageous claims, use deceptive testimonials, use high-pressure upselling, and/or use fake testimonials; (with or without a written contract) offering unrealistic incentives/rewards as an inducement to purchase products or services but do not respond to any queries after the purchase

No value added services including sale or resale of a service without added benefit to the buyer and resale of government offerings without authorization or added value

Sales of online traffic or engagement

Negative response marketing and telemarketing

Predatory mortgage consulting, lending, credit repair and counseling services

Predatory investment opportunities with no or low money down

Remote technical support; mugshot publication or pay-to-remove sites; essay mills; chain letters; door-to-door sales

Any other businesses that Stripe considers unfair, deceptive, or predatory towards consumers

Adult content and services

Pornography and other mature audience content (including literature, imagery and other media) depicting nudity or explicit sexual acts

Adult services including prostitution, escorts, pay-per view, sexual massages, and adult live chat features

Adult video stores

Gentleman's clubs, topless bars, and strip clubs

Online dating services

Certain legal services

Law firms collecting funds for purposes other than legal service fee payment

Bankruptcy attorneys

Bail bonds

Firearms, explosives and dangerous materials

Guns, gunpowders, ammunitions, weapons, fireworks and other explosives

Peptides, research chemicals, and other toxic, flammable and radioactive materials

Gambling

Games of chance including gambling, internet gambling, sweepstakes and contests, fantasy sports leagues with a monetary or material prize

Games of skill including video game and mobile game tournaments/competitions, card games, board games with a monetary or material prize

To process payments for an entry/player fee that promises the entrant/player to win a prize in money or money's worth, or to payout winnings of such games

Sports forecasting or odds making with a monetary or material prize

Lotteries

Bidding fee auctions

Marijuana

Cannabis products

Cannabis dispensaries and related businesses

Misuse of Stripe products

Use of Stripe products with false, manipulated, inaccurate, or misleading information regarding your identity, business entity, the nature of business, and any other information requested by Stripe (you must inform us immediately of any changes to your personal and business information)

Use of Stripe products to facilitate transactions on behalf of another undisclosed merchant or for products/services that were not disclosed in the merchant's Stripe account application

Use of Stripe principally as a virtual terminal (e.g., submitting card transactions by manually inputting card information)

Processing where there is no bona fide good or service sold, or donation accepted; card testing

Evasion of card network chargeback monitoring programs

Cross-border acquiring where the business address of the merchant is outside of the jurisdiction of the acquiring Stripe entity unless permitted under the card network rules

Sharing cardholder information with another merchant for payment cross-sell products or services

Use of Stripe intellectual property without prior written consent from Stripe; use of the Stripe name or logo including use of Stripe trade or service marks inconsistent with the Stripe Marks Usage Agreement, or in a manner that otherwise harms Stripe or the Stripe brand; any action that implies an untrue endorsement by or affiliation with Stripe

The types of businesses listed are representative but not exhaustive.

Additional Jurisdiction-Specific Prohibitions

Hong Kong	Marketing lead generation services
	Unregistered charities
India	Alcohol
	Charities
	Dating and matchmaking services
	Lobby groups, political organizations
	Mining and oil drilling
	Religious organizations
	Sex toys
	Soliciting donations or fund contributions
Japan	Animals
	C2C services outside of Stripe Connect
	Donations to individuals
	Fundraising for or financing businesses that are listed as prohibited/restricted above
	Health instruments
	Industrial waste disposal and garbage disposal devices; water purifiers
	International marriage brokerage businesses
Malaysia	Sex toys
Mexico	Adoption agencies
	Credit card and identity theft protection services
	Cross-border currency exchange services
	Debt collection agencies
	Direct marketing- travel
	Electronic cigarettes for card-not-present transactions
	Ephedrine
	Game console modification devices
	HCG weight loss
	Investment services
	Penny auctions
	Pharmaceuticals wholesale for card-not-present transactions
	Search engine optimization

	Telemedicine
	Tobacco for card-not-present transactions
Singapore	Marketing lead generation services
	Sale of ads for any products or services deemed illegal in Singapore; sales of products that facilitate payments to any of these products or services
	Sex toys
Thailand	Psychic services and fortune tellers
	Unregistered charities
	Vehicle sales
	Vitamins
	Historical artifacts
	Dating services
	Surrogacy services
	Online alcohol sales
	Timeshares
	Private investigators, protection services and detective agencies
	Soliciting donations or fund contributions
United Arab Emirates	Historical artifacts, ivory products, prison-made products
	Sex toys
United States	Extended warranties and subscriptions over one year
	Sex toys
	Unregistered charities

Restricted Businesses

You must not use Stripe's services for the following activities, unless you have received our prior written approval. Restricted Business categories may be imposed through card network rules, requirements of financial partners, or due to compliance and legal obligations. If your business falls into one of the restricted categories, please **contact us.** We are here to help!

Regulated industries such as:

Financial products and services

- Investment and brokerage services
- Lending services
- Buy Now Pay Later services
- Crowdfunding
- Debt collection agencies
- Insurance services including medical benefit packages
- Money transmitters, currency exchange services and other money services businesses
- Neobanks / challenger banks
- Other financial institutions

Government services

- Government grants
- Embassy, foreign consulate, or other foreign governments

Cannabidiol (CBD)

- CBD products containing negligible amounts of THC

Pharmaceuticals, medical devices and telemedicine

- Online pharmacies
- Prescription-only products including card-not-present pharmaceuticals
- Prescription-only and regulated medical devices
- Telemedicine and telehealth services

Tobacco

- Tobacco products including e-cigarettes and e-liquid

Others

- Credit card and identity theft protection services
- Other age restricted goods or services

Businesses that may pose elevated financial risk such as:

Travel

- Travel reservation services and clubs

- Airlines and cruises
- Timeshare services

Non-fiat currency and stored value

- Virtual and cryptocurrencies, non-fungible tokens (NFTs), and mining services (for crypto and NFT supportability and availability by region, please see this support doc)
- Prepaid phone cards, sim cards, and phone services
- Sale of stored value or credits maintained, accepted and issued by anyone other than the seller
- Sale of in-game currency or game items, unless the merchant is the operator of the virtual world

Business models that may be particularly prone to abuse by 'bad actors' such as:

Multi-level marketing

- Businesses where sellers get their revenue both from selling items and from signing up new sellers
- Network marketing and referral marketing programs
- Shipping and forwarding brokers

Shipping

- Shipping brokers
- Forwarding brokers
- Drop shipping

Others

- Charity sweepstakes and raffles for the explicit purpose of fundraising

The types of businesses listed are representative but not exhaustive.

Check out this blog to learn more about Stripe's approach to prohibited businesses and why some businesses aren't allowed to use Stripe's services.

Additional Product-Specific Prohibitions

Stripe Issuing

You must not use Stripe Issuing for the following activities.

Consumer use

Consumer use of Stripe Issuing is when an Issuing card is created to fully or partially enable payments for personal, family or household use, including but not limited to:

- Providing a payment method loaded with/that accesses consumer funds
- Cards that disburse payroll or payouts
- Any other use that directly or indirectly enable payments using the consumer's funds

International use

When you sign up for Stripe Issuing, you share with Stripe the location of your business, the physical address of your beneficial owners, and the jurisdiction in which your business is registered. Stripe requires that the physical location of your business, its jurisdiction of registration, and the physical address of at least one of your beneficial owners all match. Furthermore, you must use Issuing cards primarily in the same jurisdiction

Lending use

You may not use Stripe Issuing as a method to extend credit to your customers using your own funds, unless you have the appropriate licensing to do so and you have received express consent from Stripe to use Issuing for that purpose.

Other abusive use

Any other abusive use of Stripe Issuing, including but not limited to:

- Using Issuing cards to abuse free trial products at scale
- Using Issuing cards to buy in-demand items or services with the sole intent to sell them for profit. (e.g. retail scalping)
- Using Issuing cards for any other illegitimate purposes

Noncompliance:

As a user of Stripe Issuing, you are required to comply with our compliance guidelines and may at times be asked by our compliance teams to update your marketing materials or aspects of your user experience. This helps us ensure you and Stripe are continuing to comply with the Federal and State laws and regulations that govern the use of these financial products. Failure to comply within the requested timeframes may result in closure of your Stripe account.

Inactivity:

If there is inactivity on all cards associated with an account for a period of 12 consecutive months, Stripe will automatically close your Issuing account.

Integration Type:

If you plan to enable your customers to use Stripe Issuing for purposes of creating cards for your customers' employees or contractors, you must implement Stripe Issuing on Connect. For example, if you are a platform that wants to enable your customers to create cards for their employees to use for business travel or marketing expenses, you must create a

Connect Account for each of your customers. Please consult Stripe if you have any questions regarding the correct integration type for your business.

- Stripe Services Agreement
- Stripe Connected Account Agreement
- Stripe Payments Company Terms
- Acquirer Terms
  - Cross River Bank
  - PNC Bank
  - Wells Fargo Bank
- Issuing Bank Terms
- Payment Method Terms
- User Bank Debit Authorizations
- Restricted Businesses
- Other Products and Programs
  - Stripe Terminal Device EULA
  - Stripe Terminal Purchase Terms
  - Stripe Terminal Reseller Terms
  - Stripe Atlas Agreement
  - Stripe Climate Contribution Terms
- Stripe Apps
  - App Developer Agreement
  - App Marketplace Agreement
- Privacy
  - Privacy Policy
  - Cookies Policy
  - Privacy Shield Policy
  - Service Providers List
  - Data Processing Agreement
  - Stripe Privacy Center
- Intellectual Property
  - Intellectual Property Notice
  - Marks Usage
- E-SIGN Disclosure
- Licenses

stripe

United States

English (United States)

Products

Atlas
Billing
Capital
Checkout
Climate
Connect
Corporate Card
Data Pipeline
Elements
Financial Connections
Identity
Invoicing
Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Solutions

Enterprises
SaaS
Marketplaces
Creator Economy
Finance Automation
Platforms
Ecommerce
Crypto
Embedded Finance
Global Businesses

Integrations & Custom Solutions

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Resources

Support Center
Support Plans
Guides
Customer Stories
Blog
Annual Conference
Contact Sales
Privacy & Terms
Licenses
COVID-19
Sitemap
Cookie Settings
Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

Privacy Policy

Last updated: January 24, 2023

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. People use our services to enable their purchases and businesses of all sizes use our technology and services to accept payments, send payouts, and manage their businesses online. Stripe wants to be clear about our use of the Personal Data that is entrusted to us.

This Privacy Policy ("Policy") describes the "Personal Data" that we collect about you, how we use it, how we share it, your rights and choices, and how you can contact us about our privacy practices. This Policy also outlines your data subject rights, including the right to object to some uses of your Personal Data by us. Please visit the **Stripe Privacy Center** for more information about our privacy practices.

"Stripe", "we", "our" or "us" means the Stripe entity responsible for the collection and use of Personal Data under this Privacy Policy. It differs depending on your jurisdiction. **Learn More**.

"Personal Data" means any information that relates to an identified or identifiable individual, and can include information that you provide to us and that we collect about you, such as when you engage with our Services (e.g. device information, IP address).

"Services" means the products and services that Stripe indicates are covered by this Policy, which may include Stripe-provided devices and apps. Our "Business Services" are Services provided by Stripe to entities ("Business Users") who directly and indirectly provide us with "End Customer" Personal Data in connection with those Business Users' own business and activities. Our "End User Services" are those Services which Stripe provides directly to people (rather than entities) for their own use.

"Sites" means Stripe.com and the other websites, apps and online services that Stripe indicates are covered by this Policy. Collectively, we refer to Sites, Business Services and End User Services as "Services".

Depending on the context, "you" means End Customer, End User, Representative or Visitor:

> When you directly use an End User Service for your personal use (such as when you sign up for Link, or make a payment to Stripe Climate in your personal capacity), we refer to you as an "End User."

When you do business with, or otherwise transact with, a Business User (e.g. when you buy a pair of shoes from a merchant that uses **Stripe Checkout** for payment processing) but are not directly doing business with Stripe, we refer to you as an "End Customer."

When you are acting on behalf of an existing or potential Business User (e.g. you are a founder of a company, administer an account for a merchant who is a Business User, or receive an employee credit card from a Business User using Stripe Issuing), we refer to you as a "Representative."

When you visit a Site without being logged into a Stripe account or otherwise communicate with Stripe, we refer to you as a "Visitor." (e.g. you send Stripe a message asking for more information because you are considering being a user of our products).

Depending on the activity, Stripe acts as a "data controller" and/or "data processor (or service provider)" and for more information about this and on the Stripe entity that is responsible under this Policy, see **here**.

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

Our collection and use of Personal Data changes depending on whether you are acting as End User, End Customer, Representative or Visitor and our different Services. For example, if you are the sole owner of a business (i.e., sole proprietorship), we may collect Personal Data to onboard your business, but you may also be an End Customer that purchased goods from another Business User that uses Stripe's Services for payment processing and you may also be an End User who uses Link to make those purchases.

"**Transaction Data**" as used in this Privacy Policy includes Personal Data, and may include the following: your name, email address, billing address, shipping address, payment method information (such as credit or debit card number, bank account information or payment card image selected by you), merchant and location, purchase amount, date of purchase, and in some cases, some information about what you have purchased and your phone number and past purchases.

1.1 End Users

We provide End User Services where we do not act as a service provider or processor to Businesses but instead provide the Services directly to you for your personal use (e.g. Link). We provide more information about our collection, use and sharing of Personal Data in our Privacy Center, including the legal bases which we rely on for using (processing) your Personal Data.

a. Personal Data that we collect about End Users

Using Link or Connecting your Bank Account. Stripe offers you the opportunity to store your payment methods with Stripe so that you can conveniently use it across merchants who are our Business Users ("Link" was formerly known as "Remember Me"). When you opt in to Link, you agree to let us store your Personal Data such as your payment method so that you can more readily make purchases through Link with Business Users of our payment processing Business Services (e.g. name, contact information, payment method details (e.g. card number, cvc, and expiration date)). When you choose to pay with Link, we will also collect Transaction Data related to your transactions. Learn More.

If you choose to share bank account information (including for use in Link) with us, Stripe will periodically collect and process your account information (e.g. bank account owner information, account balances, account number and details, account transactions and, in some cases, credentials). With your separate permission, we will share this Personal Data with Business Users that you choose. You can ask us to stop collecting and sharing this information. Learn More.

With your separate permission, we will share contact information (e.g. shipping address, billing address and phone number) with Business Users that you do business with.

Paying Stripe. If you are buying goods or services directly from Stripe, we receive Transaction Data. For example, when you make a payment to Stripe Climate, we will collect contact information, payment method information, and information about that transaction.

I**dentity/Verification Services.** We provide an identity verification service that automates comparing an identity document with your image (e.g., selfie). You may choose to opt-in to allow us to store that verification for future use across other merchants and/or separately consent to letting us use your biometric data to improve our verification technology. You can also ask us to stop providing you these services. Learn More.

More. Please see below for information about additional types of Personal Data that we may collect about End Users, including about your online activity and how you engage with our End User Services.

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

Services. We use your Personal Data to provide the End User Service to you, including security, sanctions screening, delivery, support, personalization (e.g. language preferences and settings choices) and messages related to the End User Service (e.g. communicating Policy updates and information about our Services). For example, we will use Personal Data to assess whether your use of Link to make a payment with a merchant is authorized by you (and not a bad actor) and likely to be successfully authorized by the payment method you choose to use when you choose to make purchases with Link.

Our Business Users. When you choose to connect your financial account with Stripe you may also choose to share account information with Business Users that you do business with. These Business Users will have their own privacy policies which describe how they use that information.

Transactions. For payment transactions with Link, End User Personal Data is shared with others to enable or "process" the transaction. For example, when you choose to use a payment method for the transaction with Stripe or with Link (e.g. credit

card, debit card, buy now pay later, or direct debit), the third party provider of your payment method will receive Transaction Data that includes your Personal Data. When you use Link, the merchant you choose to do business with will also receive Transaction Data that includes your Personal Data and, with your separate consent, your bank account information. Please review the privacy policies of your payment method and the merchants who you choose to learn more about their processing of your Personal Data.

Fraud Detection and Loss Prevention. We use your Personal Data collected across our Services (e.g. Stripe Radar) to detect fraud and prevent financial losses for you, us, and our Business Users and financial partners, including to detect unauthorized purchases. Learn More. We may provide Business Users and financial partners (including card issuers, payment methods and others involved in payment processing activities) that use our fraud Business Services with Personal Data about you (including your attempted transactions) so that they can assess the associated fraud or loss risk with a transaction. You can 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 here.

Advertising. We may use your Personal Data to assess your eligibility for, and offer you, other End User Services or promote existing End User Services. Where allowed by law (including with your opt-in consent where required), we use and share End User Personal Data with others so that we may market our End User Services to you, including through interest-based advertising. See our Cookie Policy.

> We do not sell or share End User Personal Data with third parties for marketing or advertising their products without your separate consent.

More. Please see below for information about additional ways in which we may use and share your Personal Data.

1.2 End Customers

Stripe offers Business Services to our Business Users (e.g. payment processing through in-person or online checkout, or processing pay-outs for those Business Users). When we are acting as a Business User's service provider (also known as a data processor), we will process Personal Data in accordance with the terms of our agreement with the Business User and the Business User's lawful instructions (e.g. when we process a payment for a Business User because you bought a product from them) or they instruct us to send funds to you.

Business Users are responsible for making sure that their End Customers' privacy rights are respected, including ensuring appropriate disclosures about data collection and use that happens in connection with their products and services. If you are an End Customer, please refer to the privacy policy or notice of the Business User you choose to do business with for information regarding their privacy practices, choices and controls. We provide more information about our collection, use and sharing of Personal Data in our Privacy Center, including the legal bases which we rely on for using (processing) your Personal Data.

a. Personal Data that we collect about End Customers

Transaction Data. If you are an End Customer, when you make payments to, get refunds from, begin a purchase, make a donation or otherwise transact with a Business User that uses us to provide payment processing Business Services, we will receive Transaction Data. We may also receive your transaction history with the Business User. Learn More. Moreover, we may obtain information typed into a checkout form, even if you choose not to complete the form or purchase with the Business User. Learn More.

Identity/Verification Information. Stripe provides a verification and fraud prevention Service that allows a Business User to verify Personal Data about you, such as your age (when purchasing age restricted goods) or your authorization to use a payment method. As part of these Services, you will be asked to share Personal Data with us for this purpose (e.g., your government ID, your image (selfie), and Personal Data you input or that is apparent from the physical payment method (e.g.

credit card image)). To protect against fraud, we may compare this information with information about you we collect from Business Users, financial partners, business partners, identity verification services, publicly available sources, and other third party service providers and sources so that we can assess whether the person is likely to be you or a person purporting to be you. Learn More.

More. Please see below for information about additional types of Personal Data that we may collect, including your online activity.

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

To provide our Business Services to our Business Users, we use Personal Data, and share Personal Data of a Business User's End Customers with the Business User. Where allowed, we also use End Customers' Personal Data for Stripe's own purposes to secure, improve and provide our Business Services and prevent fraud, loss and other harms as described below.

Payments and Accounting. We use your Transaction Data to provide our Payments related Business Services to Business Users, including to process online payment transactions, to calculate applicable sales tax, to invoice and bill, and to help them calculate their revenue, pay their bills and perform accounting tasks. Learn More. We may also use Personal Data to provide and improve our Business Services.

For payment transactions, your Personal Data is shared with a number of parties in connection with your transaction. Because we act as a service provider or processor, we share Personal Data to enable the transaction. For example, when you choose to use a payment method for the transaction (e.g. credit card, debit card, buy now pay later, or direct debit), your payment method will receive the Transaction Data that includes your Personal Data. Please review your payment method's privacy policy to learn more about how they use and share this information.

The merchant you choose to do business with will also receive Transaction Data that includes your Personal Data and the merchant may share that Personal Data with others. Please review your merchant's privacy policy to learn more.

Financial Services. Some of our Business Users use our Services in order to offer financial services to you, through Stripe or its financial partners. For example, they may provide a card product that enables you to purchase goods and services. These cards may carry the Stripe brand, bank partner brand and/or the brands of Business Users. In addition to any Transaction Data we may produce or receive when these cards are used for purchases, we will also receive and use your Personal Data in order to provide and manage these products. Please also see the privacy policies of the Business User and our bank partners, if applicable, associated with the financial service (whose brands may be shown on the card).

I**dentity/Verification Services.** We use Personal Data about your identity, including information provided by you and our service providers, to perform verification Services for Stripe or for the Business Users that you are doing business with, to reduce fraud and enhance security. If you provide a "selfie" along with an image of your identity document, we will use technology to compare and calculate whether they match and you can be verified. Learn More.

Fraud Detection and Loss Prevention. We use your Personal Data collected across our Services (e.g. Stripe Radar) to detect and prevent losses for you, us, our Business Users and financial partners. We may provide Business Users (including card issuers, payment methods and others involved in payment processing activities) that use our fraud Business Services with Personal Data about you (including your attempted transactions) so that they can assess the fraud or loss risk associated with a transaction. You can learn more about how we may use technology to assess the fraud and loss risk associated with an attempted transaction and what information we may share with Business Users about such risks here and here.

Our Business Users (their Authorized Third Parties). We share Personal Data of End Customers with their respective Business Users and with parties directly authorized by those Business Users to receive Personal Data. This includes sharing Personal Data of End Customers with Business Users when a Business User authorizes a third party application provider to access its Stripe account using Stripe Connect. For example, when the Business User uses Identity Services to

verify an End Customer's identity, Stripe shares with the Business User the information, documents or photos provided by the End Customer to verify their identity. The Business Users you choose to do business with may further share your Personal Data to third parties they authorize (e.g. other third party service providers). Please review their privacy policy to learn more.

Advertising by Business Users. If you have begun a purchase, we share Personal Data with that Business User in connection with our provision of Services and that 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 your merchant's privacy policy to learn more, including your rights to stop their use of your Personal Data for marketing purposes.

> We do not use, sell or share End Customer Personal Data for our marketing or advertising, or for marketing and advertising by third parties who are not the Business User with which you have transacted or attempted to transact.

More. Please see below for information about additional ways in which we may use and share your Personal Data.

1.3 Representatives

To provide Business Services, we collect, use and share Personal Information from Representatives of Business Users (e.g. a business owner). We provide more information about our collection, use and sharing of Personal Data in our Privacy Center, including the legal bases which we rely on for using (processing) your Personal Data.

a. Personal Data that we collect about Representatives

Registration and Contact Information. If you register for a Stripe account for a Business User (including incorporation of a Business), we collect your name and account log-in credentials. If you register for an event that Stripe organizes or attends or if you sign up for Stripe communications, we collect your registration and profile information. If you are a Representative or Representative of a potential Business User, we receive your Personal Data from third parties (including data providers) in order to advertise to, market and communicate with you as described further below and in Section 2. We may also associate a location with you in order to assess which Services or information may be useful to you. Learn More.

Identification Information. If you are an owner of a Business User or you are expected to be a shareholder, officer or director of a Business User, we require that you provide your contact details, such as name, postal address, telephone number, and email address to fulfill our financial partner and regulatory requirements. We will directly (and through others) collect Personal Data about you, such as your ownership interest in the Business User, your date of birth and government identifiers associated with you and your Business User (such as your social security number, tax number, or Employer Identification Number). You may also choose to provide bank account information.

More. Please see below for information about additional types of Personal Data that we may collect, including about online activity.

b. How we use and share Personal Data of Representatives

We generally use Personal Data of Representatives to provide the Business Services to the associated Business Users, as well as for the purposes described below.

Business Services. We use and share Personal Data of Representatives with Business Users to provide the Services you (or the Business User you are associated with) have requested.

> In some cases our Business Service will require us to submit your Personal Data to a government entity (e.g. incorporating a business, or paying applicable sales tax). For our tax Business Services, we may use your Personal Data to file taxes on behalf of your associated Business User. For our Atlas business incorporation services, we may

use your Personal Data to submit forms to the IRS on your behalf and to file documents with other governmental authorities (e.g. articles of incorporation in your state of incorporation).

We share data with parties directly authorized by a Business User to receive Personal Data (e.g. financial partners servicing the financial product, or third party apps or services the Business User uses in conjunction with our Business Services). For example, providers of payment methods (e.g., Visa, WeChat Pay) will require merchant onboarding information for the Business Users that accept their payment methods, and Stripe will provide required onboarding information (including Personal Data of Representatives) to those financial partners. In some cases, these payment method providers will be located outside your home country for example WCP, AliPay, Block, Klarna Bank AB. Learn More.

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

If you are a Business User and have chosen a name that includes Personal Data (e.g. a sole proprietorship or family name in a company name), we will share and use that information as any company name in connection with the provision of our Services (e.g. including it on receipts and other descriptions identifying financial transactions).

Advertising. Where allowed by applicable law, we use and share Representative Personal Data with others so that we may advertise and market our Services to you. Subject to applicable law (including any consent requirements), we may advertise to you through interest-based advertising and emails and seek to measure the effectiveness of our ads. See our Cookie Policy. We do not sell or share Representative Personal Data to others for their advertising purposes.

More. Please see below for information about additional ways in which we may collect, use and share your Personal Data.

1.4 Visitors

We collect, use and share Personal Data of Visitors (who are not End Users, End Customers or Representatives). We provide more information about our collection, use and sharing of Personal Data in our Privacy Center, including the legal bases which we rely on for using (processing) your Personal Data.

a. Visitor Personal Data that we collect

When you visit our Sites, we will receive your Personal Data either from you providing it to us or through our use of cookies and similar technologies. See our Cookie Policy.

Forms. When you choose to fill in a form on the Site or on third party websites featuring our advertising (e.g. LinkedIn or Facebook), we will collect the information included in the form (e.g. your contact information and other information about your question related to our Services). We may also associate a location with your visit. Learn More.

More. Please see below for information about additional types of Personal Data that we may collect, including about online activity.

b. How we use and share visitor Personal Data

Personalization. We use information about you that we gather from cookies and similar technologies to measure engagement with the content on the Sites, to improve relevancy and navigation, to personalize your experience (e.g. language and relevant geography) and to tailor content about Stripe and our Services to you. For example, because not all of our Services are available in all regions, so we may tailor our answers for your region.

Advertising. As allowed by law, we use and share Visitor Personal Data with others so that we may advertise and market our Services to you. Subject to applicable law (including any consent requirements), we may advertise our Services to you through interest-based advertising and emails, and seek to measure the effectiveness of our ads. See also our Cookie Policy. We do not sell or share Visitor Personal Data to others for their advertising purposes.

Engagement. When visitors engage with our stripe.com site, we will use information we collect about and through your devices in order to provide the opportunity to engage in conversations or with chatbots to address your questions.

More. Please see below for information about additional ways in which we may collect, use and share your Personal Data.

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

In addition to the ways we collect, use and share Personal Data that are described above, we also process your Personal Data as follows:

a. Personal Data Collection

Online Activity. Depending on the Service you use and the Business Users' implementation of our Business Services, we will collect information about:

Devices and browsers across our Sites and third-party websites, apps and other online services ("**Third-Party Sites**"),

Usage data associated with those devices and browsers and how you've engaged with our Services, including IP address, plug-ins, language used, time spent on Sites and Third-Party Sites, pages visited, links clicked, payment methods used, and the pages that led or referred you to Sites and Third-Party Sites. For example, activity indicators, like mouse activity indicators, to help us detect fraud. Learn More. Please also see our Cookie Policy.

Communication and Engagement Information. We will collect any information you choose to provide to us, for example, through support tickets, emails or social media. When you respond to Stripe emails or surveys, we collect your email address, name and any other information you choose to include in the body of your email or responses. If you contact us by phone, we will collect the phone number you use to call Stripe, as well as other information you may provide during the call. We will also collect your engagement data such as your registration for, attendance of, or viewing of Stripe events and other interaction with Stripe personnel.

Forums and Discussion Groups. Where our Sites allow you to post content, we will collect Personal Data that you provide in connection with the post.

b. Personal Data Usage. In addition to the Personal Data usage described above, we use Personal Data in the following ways:

Improving and Developing our Services. We use analytics on our Sites to help us analyze your use of our Sites and Services and diagnose technical issues. To learn more about the cookies that may be served through our Sites and how you can control our use of cookies and third-party analytics, please see our Cookie Policy. We also collect and process Personal Data through our different 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 relevant and more useful to you. Learn More.

Communications. We will use the contact information we have about you to perform the Services, which may include sending codes via SMS to authenticate you. Learn More. If you are an End User, Representative or Visitor, we may

communicate with you using the contact information we have about you (e.g. using email, phone, text message or videoconference) to provide information about our Services and our affiliates' services, invite you to participate in our events or surveys, or otherwise communicate with you for our marketing purposes, provided that we do so in accordance with applicable law, including any consent or opt-out requirements. For example, when you submit your contact information to us or when we collect your business contact details through our participation at trade shows or other events, we may use the information to follow-up with you regarding an event, send you information that you have requested on our products and services and include you on our marketing information campaigns.

Social Media and Promotions. If you choose to submit Personal Data to us to participate in an offer, program or promotion, we will use the Personal Data you submit to administer the offer, program or promotion. We will also use that Personal Data and Personal Data you make available on social media to market to you unless we are not permitted to do so.

Fraud Prevention and Security. We collect and use Personal Data to help us to detect and manage the activity of fraudulent and other bad actors across our Services, to enable our fraud detection Business Services, and to otherwise seek to secure our Services and transactions against unauthorized access, use, modification or misappropriation of Personal Data, information and funds. In connection with fraud and security monitoring, prevention, detection, and compliance activities for Stripe and its Business Users, we receive information from service providers (including credit bureaus), third parties, and the Services we provide. We may collect information from you, and about you, from Business Users, financial parties and in some cases third parties. For example, to protect our Services, we may receive information from third parties about IP addresses that malicious actors have compromised. Learn More. This Personal Data (e.g. name, address, phone number, country) helps us to confirm identities, run credit checks subject to applicable law and prevent fraud. We may also use technology to assess the fraud risk associated with an attempted transaction by an End Customer or End User with a Business User or financial partner.

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, export control and prohibitions on doing business with restricted persons or in certain business areas and other legal obligations. Learn More. We strive to make our Services safe, secure and compliant, and the collection and use of Personal Data is critical to this effort. For example, we may monitor patterns of payment transactions and other online signals and use those insights to reduce the risk of fraud, money laundering and other activity that is harmful to Stripe, our End Users and their End Customers.

Minors. The Services are not directed to minors, including children under the age of 13, and we request that they not provide Personal Data through the Services. In some countries, we may impose higher age limits as required by applicable law.

c. **Personal Data Sharing**. In addition to the ways described above, we share Personal Data in the following ways:

Stripe Affiliates. We share Personal Data with other Stripe affiliated entities. When we share with these entities, it is for purposes identified in this Policy.

Service Providers or Processors. In order to provide Services to our Business Users and End Users and to communicate, market and advertise to Visitors, Representatives and End Users regarding our Services, we will rely on others to provide us services. Service providers provide a variety of critical services, such as hosting (storing and delivering), analytics to assess the speed, accuracy and/or security of our Services, identity verification, customer service, email and auditing. We authorize such service providers to use or disclose the Personal Data that we make available to perform services on our behalf and to comply with applicable legal requirements. We require such service providers to contractually commit to protect the security and confidentiality of Personal Data they process on our behalf. Our service providers are predominantly located in the European Union, the United States of America and India. Learn More.

Financial Partners. "Financial Partners" are financial institutions that we partner with to offer the Services (including payment method acquirers, banks and payout providers). We share Personal Data with certain Financial Partners to provide the Services to the associated Business Users and to offer certain Services in partnership with our Financial Partners. For example, we share certain Personal Data of Representatives (e.g. loan repayment data and contact

information) with institutional investors who purchase or provide credit secured by the Capital loans that we have made to the associated Business Users.

Others with Consent. In some cases we may not provide a service, but instead refer you to, or enable you to engage with, others to get services (e.g. professional services firms that we partner with to deliver Atlas). In these cases, we will disclose the identity of the third party and the information that will be shared with them and seek your consent to share the information.

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

Compliance and Harm Prevention. We share Personal Data as we believe necessary: (i) to comply with applicable law, (ii) to comply with rules imposed by a payment method in connection with use of that payment method (e.g. network rules for Visa); (iii) to enforce our contractual rights; (iv) to secure or protect the Services, rights, privacy, safety and property of Stripe, you or others, including against other malicious or fraudulent activity and security incidents; and (v) to respond to valid legal process 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 data

For the purposes of the General Data Protection Regulation, we rely upon a number of legal bases to enable our processing of your Personal Data. For more information, see here.

a. Contractual and Pre-Contractual Business Relationships. We process Personal Data for the purpose of entering into business relationships with prospective Business Users and End Users and to perform the respective contractual obligations with them. Activities include:

Creation and management of Stripe accounts and Stripe account credentials, including the evaluation of applications to commence or expand the use of our Services;

Creation and management of Stripe Checkout accounts;

Accounting, auditing, and billing activities; and

Processing of payments, including fraud detection, loss prevention, optimizing valid transactions, communications regarding such payments, and related customer service.

b. Legal Compliance. We process Personal Data to verify the identity of individuals and entities in order to comply with fraud monitoring, prevention and detection obligations, laws associated with the identification and reporting of illegal and illicit activity, such as "Anti-Money Laundering ("AML") and Know-Your-Customer ("KYC")" obligations, and financial reporting obligations. For example, we may be required to record and verify a User's identity for the purpose of compliance with legislation intended to prevent money laundering and financial crimes. These obligations are imposed on us by the operation of law and may require us to report our compliance to third parties, and to submit to third party verification audits.

c. Legitimate Interests. Where allowed under applicable law, we rely on our legitimate business interests to process Personal Data about you. The following list sets out the business purposes for which we have a legitimate interest in processing your data:

- Detect, monitor and prevent fraud and unauthorized payment transactions;
- Mitigate financial loss, claims, liabilities or other harm to End Customers, End Users, Business Users and Stripe;
- Determine eligibility for and offer new Stripe products and services Learn More;
- Respond to inquiries, send Service notices and provide customer support;
- Promote, analyze, modify and improve our Services, systems, and tools, and develop new products and services, including reliability of the Services;
- Manage, operate and improve the performance of our Sites and Services by understanding their effectiveness and optimizing our digital assets;
- Analyze and advertise our Services, and related improvements;
- Conduct aggregate analysis and develop business intelligence that enable us to operate, protect, make informed decisions, and report on the performance of, our business;
- Share Personal Data with third party service providers that provide services on our behalf and business partners which help us operate and improve our business Learn More;
- Enable network and information security throughout Stripe and our Services; and
- Share Personal Data among our affiliates.

d. Consent. We may rely on consent to collect and process Personal Data as it relates to how we communicate with you and for the provision of our Services such as Link, Financial Connections, Atlas and Identity. When we process data based on your consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing based on such consent before the consent is withdrawn.

4. Your rights and choices

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 no longer want to receive marketing-related emails from us, you may opt-out via the unsubscribe link included in such emails or as described here. We will try to comply with your request(s) as soon as reasonably practicable. Please note that if you opt-out of receiving marketing-related emails from us, (i) we retain the right to communicate to you regarding the services you receive (e.g. support and important legal notices) and (ii) our Business Users may still send you messages and/or direct 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 described here with regard to the Personal Data we control about you:

- The right to request confirmation of whether Stripe processes Personal Data relating to you, and if so, to request a copy of that Personal Data;
- The right to request that Stripe rectify or update your Personal Data that is inaccurate, incomplete or outdated;
- The right to request that Stripe erase your Personal Data in certain circumstances 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 considers another request that you have submitted (including a request that Stripe make an update to your Personal Data);
- The right to request that we export your Personal Data that we hold to another company, where technically feasible;
- Where the processing of your Personal Data is based on your previously given consent, you have the right to withdraw your consent at any time;
- Where we process your information based on our legitimate interests, you may also have the right to object to the processing of your Personal Data. Unless we have compelling legitimate grounds or where it is needed for legal reasons, we will cease processing your information when you object. Learn More.
- The right not to be discriminated against for exercising these rights; and/or
- The right to appeal any decision by Stripe relating to these rights.

You may have additional rights regarding your Personal Data under applicable law. For example, see Jurisdiction-specific provisions section under California below.

c. Process for exercising your data protection rights

To exercise your data protection rights please also see the Stripe Privacy Center or contact us as described below.

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 Personal Data covered by this Policy against unauthorized access, destruction, loss, alteration or misuse. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure.

To help us protect Personal Data, where you have an account with Stripe, we encourage you to use a strong password, protect that password from unauthorized use and not use the same log-in credentials (e.g. password) for your Stripe accounts as you do with other services or accounts. If you have reason to believe that your interaction with us is no longer secure (e.g. you feel that the security of your Stripe account has been compromised), please contact us immediately. Learn More.

We retain your Personal Data as long as we are providing the Services to you or our Business Users (as applicable) or for a period during which we reasonably anticipate providing the Services. Even after we stop providing Services directly to

you or a Business User with which you are doing business, and even if you close your Stripe account or complete a transaction with a Business User, we may retain your Personal Data:

- to comply with our legal and regulatory obligations.
- to enable fraud monitoring, detection and loss prevention activities.
- to comply with our tax, accounting, and financial reporting obligations
- where required by our contractual commitments to our financial partners (and where data retention is mandated by the payment methods you used).

In cases where we keep Personal Data, we do so in accordance with any limitation periods and records retention obligations that are imposed by applicable law. Learn More.

6. International data transfers

We are a global business. We may transfer your Personal Data to countries other than your own country, including to the United States. These countries may have data protection rules that are different from 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 see Stripe Privacy Center for more information. Where applicable law requires a data transfer mechanism, we use one or more of the following:

- Transfers to certain countries or recipients that are recognised 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.
- or other legal methods available to us under applicable law.

While Stripe, Inc. remains self-certified under the E.U.-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield, it is not currently relying on these frameworks for the transfer of Personal Data to the United States.

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

Brazil. To exercise your rights, you may **contact our DPO**. Brazilian residents, to 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) and "Personal Data" includes "personal information" as defined under PIPEDA.

EEA and UK. To exercise your rights, you may **contact our DPO**. If you are a resident of the EEA or if we have identified Stripe Payments Europe Limited as your data controller, and you believe our processing of your information is not in line with the General Data Protection Regulation (GDPR), you may direct your questions or complaints to the Irish Data Protection Commission. If you are a resident of the UK, you may direct your questions or concerns to the UK Information Commissioner's Office. Where Personal Data is used for regulated financial activities in Europe, Stripe Payments Europe Limited and Stripe local regulated entities (defined as those who are licensed, authorized or registered by a Local Regulatory Authority) are considered joint controllers. Learn More.

India. If you have any questions or complaints regarding the processing of your Personal Data in India, please contact our Nodal and Grievance Officer here. Learn More.

Indonesia. As used 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 "Personal Data" includes "personal data" as defined under such laws.

Japan. When we transfer Personal Data of data subjects in Japan to jurisdictions that are 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.

Malaysia. If you have any questions or complaints about this Policy, please **contact our DPO**.

Switzerland. As used 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**.

Thailand. If we process your Personal Data due to a legal obligation or contractual right and you do not provide us with personal Information, we may not be able to lawfully provide you services.

United States - California. If you are a consumer located in California, we process your personal information in accordance with California law (e.g. the "CCPA"). For specific details, please see here. Stripe uses cookies, including advertising cookies, as described in our Cookie Policy.

Your Rights and Choices. As a California consumer and subject to certain limitations under the CCPA, you have choices regarding our use and disclosure of your personal information (**learn more** about data subject rights metrics). In addition to the above rights (see **here**), please note these other California-specific rights:

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: We do not sell "Personal Information" as defined by the CCPA and have not done so in the past 12 months. **Learn more**.

Exercising the right to limit the use or sharing of Sensitive Personal Information: we do not sell or share Sensitive Personal Information as defined by the CCPA and have not done so in the past 12 months. Learn more about our collection and use of Sensitive Personal Information **here**.

Right to opt-out of sharing of cross-context behavioral advertising. Learn more **here** and **here**.

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. 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. 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 provided the authorized agent permission to submit the request.

Do Not Track and signals. **Learn more** about how we honor "do not track" and other signals.

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.

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

- Cross River Bank
- PNC Bank
- Wells Fargo Bank

Issuing Bank Terms

Payment Method Terms

User Bank Debit Authorizations

Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

Cookie Policy

Last updated: April 14, 2022

This cookie policy describes how Stripe ("**Stripe**") uses "cookies" and other similar technologies, in connection with our Site and Services. To learn more about Stripe-affiliated websites, please see section 4 below. Any capitalized term used and not otherwise defined below has the meaning assigned to it in the Privacy Policy.

1. What is a Cookie?

Cookies are small text files that are stored in a computer's browser directory. They help site providers with things like understanding how people use a site, remembering a User's login details, and storing site preferences.

2. Does Stripe use Cookies?

Yes. We use cookies in accordance with our **Privacy Policy** to:

ensure that our Services function properly,

detect and prevent fraud,

understand how visitors use and engage with our Site, and

analyze and improve Services.

3. Who sets cookies when I use Stripe's Site?

There are two main types of cookies that can be set:

First party cookies: these cookies are placed and read by Stripe directly when you use our Services,

Third party cookies: these cookies are not set by Stripe, but by other companies, like Google or Facebook, for site analytics purposes. See further details **below** on how to manage these cookies.

4. How Stripe Uses Cookies

Cookies play an important role in helping us provide effective and safe Services. Below is a description of the commonly used cookie types and the purposes that apply to them. Each section references Stripe's **Cookie Settings Dashboard**, where you can find more information about each cookie, and exercise your choices.

For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly.

Necessary Cookies

Some cookies are essential to the operation of our Site and Services and make it usable and secure by enabling basic functions like page navigation and access to secure areas of the Site. We use those cookies in a number of different ways, including:

Authentication. To remember your login state so you don't have to log in as you navigate through our Site and dashboard.

Fraud Prevention and Detection. Cookies and similar technologies that we deploy through our Site help us learn things about computers and web browsers used to access the Services. This information helps us monitor for and detect potentially harmful or illegal use of our Services. For example, in order to process payments transactions for our Users, it is necessary for Stripe to collect information about the transaction and the Customer. To help secure these transactions and minimize fraud, we collect additional information through the use of cookies and other technologies in helping to identify bad actors and prevent them from making fraudulent transactions. Customers should check our Users' sites for more information about the use of Stripe cookies for fraud detection.

Security. To protect user data from unauthorized access.

Functionality. To keep our Site and Services working correctly, like showing you the right information for your selected location.

For more information, please see the **Authentication**, **Fraud Prevention**, **Security** and **Functionality** sections in the **Stripe Cookie Settings Dashboard**. For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly.

Preference Cookies

Preference cookies are used by Stripe to remember your preferences and to recognize you when you return to our Services.

For more information, please see the **Preferences** section in the Stripe **Cookie Settings Dashboard**. For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly.

Analytics Cookies

Analytics cookies help us understand how visitors interact with our Services. We use those cookies in a number of different ways, including:

Site Features and Services. To remember how you prefer to use our Services so that you don't have to reconfigure your settings each time you log into your account.

To Analyze and Improve Our Services. To make our Site and Services work better for You. Cookies help us understand how people reach our Site and our Users' sites. They give us insights into improvements or enhancements we need to make to our Site and Services.

Pixel tags (also known as web beacons and clear GIFs). May be used in connection with some Services to, among other things, track the actions of Users (such as email recipients), measure the success of our marketing campaigns and compile statistics about usage of the Services and response rates.

Third Party Analytics. Through Google Analytics in order to collect and analyze information about the use of the Services and report on activities and trends. This service may also collect information regarding the use of other sites, apps and online resources. You can learn about Google's practices on the **Google website**. See further details below on how to manage these cookies.

For more information, please see the **Analytics** section in the Stripe **Cookie Settings Dashboard**. For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly.

Advertising Cookies

We and our service providers will use cookies and similar technologies on Stripe.com to direct Stripe ads to you through targeted advertisements for Stripe Services on other sites you visit and to measure your engagement with those ads.

For more information, please see the **Advertising** section in the Stripe **Cookie Settings Dashboard**. For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly.

5. Can I opt-out?

Yes. You can opt out of cookies through our **Cookie Settings Dashboard**, with the exception of those cookies that are necessary to provide you with our Services. For Stripe-affiliated websites, you can learn more about cookies by visiting those sites directly. Your web browser may allow you to manage your cookie preferences, including to delete and disable Stripe cookies. You can take a look at the help section of your web browser or follow the links below to understand your options. If you choose to disable cookies, some features of our Site or Services may not operate as intended.

Chrome: **https://support.google.com/chrome/answer/95647?hl=en**

Explorer: **https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies**

Safari: **https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac**

Firefox: **https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer**

Opera: **https://help.opera.com/en/latest/web-preferences/#cookies**

Stripe Services Agreement

Stripe Connected Account Agreement

Climate
Connect
Corporate Card
Data Pipeline
Elements
Financial Connections
Identity
Invoicing
Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Finance Automation
Platforms
Ecommerce
Crypto
Embedded Finance
Global Businesses

Integrations & Custom Solutions

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Blog
Annual Conference
Contact Sales
Privacy & Terms
Licenses
COVID-19
Sitemap
Cookie Settings
Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

EU-U.S. and Swiss-U.S. Privacy Shield Policy

Last updated: November 13, 2019

Stripe Inc. (“Stripe”, “we”, “our” or “us”) has subscribed to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, “Privacy Shield”). Stripe adheres to the Privacy Shield Principles including the Supplemental Principles, (collectively, the “Privacy Shield Principles”) for Personal Data received from entities in the European Economic Area (the “EEA”), the United Kingdom (“UK”) and Switzerland.

This Stripe Privacy Shield Policy (“Privacy Shield Policy”) and the **Stripe Privacy Policy** (“Privacy Policy”) describe the privacy practices that we implement for Personal Data received from the EEA, UK or Switzerland in reliance on the Privacy Shield. This Privacy Shield Policy uses terms which are defined in the Privacy Policy.

If there is any conflict between the terms in this Privacy Shield Policy and the Privacy Shield Principles as concerns the Personal Data received under the Privacy Shield, the Privacy Shield Principles shall govern to the extent of the conflict. To learn more about the Privacy Shield program visit **www.privacyshield.gov**, and to view our certification, please visit **https://www.privacyshield.gov/list**.

Privacy Shield Principles

1. and 2. Notice and Choice

Our Privacy Policy describes how we use Personal Data we receive from different sources. This Privacy Shield Policy describes how we process Personal Data covered by the Privacy Shield.

If you are a User, Stripe may act as an agent for you in relation to the Personal Data that you provide or make available to Stripe. Stripe usually will not have a relationship with your Customers. Here, the User is responsible for ensuring that Customers are provided with appropriate notice and choice with respect to their Personal Data.

In its role as a controller and as required by applicable law, Stripe generally offers individuals in the EU, UK and Switzerland (together: “EEA/UK/CH Consumers”) the opportunity to choose whether their Personal Data may be (i) disclosed to third-party controllers or (ii) used for a purpose that is materially different from the purposes for which the information was originally collected or subsequently authorized by the relevant EEA/UK/CH Consumer. To the extent required by the Privacy Shield Principles, Stripe obtains opt-in consent for certain uses and disclosures of sensitive data. EEA/UK/CH Consumers may contact Stripe as indicated below regarding the Stripe’s use or disclosure of their Personal

Data. Unless Stripe offers EEA/UK/CH Consumers an appropriate choice, Stripe uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

3. Data Integrity and Purpose Limitation

We only collect Personal Data that is relevant to providing our Services. We process Personal Data compatible with us providing the Services or as otherwise notified to you. We take reasonable steps to ensure that the Personal Data received under the Privacy Shield is needed for Stripe's Services, accurate, complete, and current.

4. Accountability for Onward Transfers

This Policy and the Privacy Policy describe how Stripe shares Personal Data.

Except as permitted or required by applicable law and in accordance with Stripe's role as a controller or processor, Stripe provides EEA/UK/CH Consumers with an opportunity to opt out of sharing their Personal Data with third-party controllers. Stripe requires third-party controllers to whom it discloses the Personal Data of EEA/UK/CH Consumers to contractually agree to (a) only process the Personal Data for limited and specified purposes consistent with the consent provided by the relevant EEA/UK/CH Consumer, (b) provide the same level of protection for Personal Data as is required by the Privacy Shield Principles, and (c) notify Stripe and cease processing Personal Data (or take other reasonable and appropriate remedial steps) if the third-party controller determines that it cannot meet its obligation to provide the same level of protection for Personal Data as is required by the Privacy Shield Principles.

Stripe may disclose Personal Data to trusted third parties as indicated in the Privacy Policy without offering an opportunity to opt out. Stripe requires that its agents and service providers that have access to Personal Data within the scope of this Privacy Shield Policy provide the same level of protection as required by the Privacy Shield Principles. We ensure that our agents process Personal Data received under the Privacy Shield in a manner consistent with our obligations under the Privacy Shield Principles, unless we prove that we are not responsible for the event giving rise to the damage.

We may also need to disclose Personal Data in response to lawful requests by public authorities, for law enforcement or national security reasons, or when such action is necessary to comply with a judicial proceeding or court order, or when otherwise required by law. We do not offer an opportunity to opt out from this category of disclosure.

5. Data Security

We use reasonable and appropriate physical, electronic, and administrative safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.

6. Access to Personal Data

Our Privacy Policy explains how you may access and/or submit requests to review, correct, update, suppress, or delete Personal Data. You can ask to review and correct Personal Data that we maintain about you by sending a written request

to **privacy@stripe.com**. We may limit or deny access to Personal Data where providing such access is unreasonably burdensome, expensive under the circumstances, or as otherwise permitted by the Privacy Shield Principles.

When Stripe acts on behalf of its Users, Stripe will assist Users in responding to individuals exercising their rights under the Privacy Shield Principles.

If you are a Customer of a User, please contact the User directly with your request to access or limit the use or disclosure of your Personal Data. If you contact us with the name of the User to which you provided your Personal Data, we will refer your request to that User and support them in responding to your access request.

7. Recourse, Enforcement and Dispute Resolution

If you have any questions or concerns, please write to us at the address listed below. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the Privacy Shield Principles.

In the event we are unable to resolve your concern, you may contact **JAMS**, which provides an independent third-party dispute resolution body based in the United States, and they will investigate and assist you free of charge. A binding arbitration option may also be available to you in order to address residual complaints not resolved by any other means. Stripe is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission ("FTC").

Contact Information

If you have any questions regarding this Privacy Shield Policy, please contact us by email at **privacy@stripe.com**, or please write to the following address:

Stripe, Inc.

354 Oyster Point Boulevard

South San Francisco, California, 94080

Attention: Stripe Legal

Changes to this Privacy Shield Policy

This Privacy Shield Policy may be changed from time to time, consistent with the requirements of the Privacy Shield and in accordance with the process described in the Privacy Policy. You can determine when this Privacy Shield Policy was last revised by referring to the "LAST UPDATED" date at the top of this page.

Stripe Services Agreement

Stripe Connected Account Agreement

stripe

Data Processing Agreement

This Data Processing Agreement only applies to you if you have a Stripe Account located in the United States, the United Kingdom, the European Economic Area and Switzerland. If you have a Stripe Account located elsewhere or would like more information on our Data Processing Agreement, please see our FAQs.

Need a copy of this Data Processing Agreement? Click here.

Last updated:

United States - June 29, 2023

United Kingdom, the European Economic Area and Switzerland - June 29, 2023

This Data Processing Agreement ("**DPA**") is subject to and forms part of your **Stripe Services Agreement** and governs Stripe's and its Affiliates' Processing of Personal Data.

1. Structure.

If your Stripe Account is located in North America or South America, you enter this DPA with Stripe, Inc. ("**SINC**"). If your Stripe Account is located elsewhere, you enter this DPA with Stripe Payments Europe, Limited ("**SPEL**"). Accordingly, references in this DPA to "Stripe" mean SINC or SPEL, as applicable. If your **Stripe Services Agreement** is with an SSA Affiliate, Stripe may engage that SSA Affiliate to Process Personal Data according to this DPA.

2. Definitions.

Capitalized terms not defined in this DPA have the meanings given to them in your **Stripe Services Agreement**.

"Approved Data Transfer Mechanism" means, as applicable, the EEA SCCs, the UK Data Transfer Addendum or any data transfer mechanism a supervisory authority approves under DP Law that is incorporated into this DPA.

"Authorized Services" means Services that a Governmental Authority licenses, authorizes or regulates.

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199.

"DP Law" means all Law that applies to Personal Data Processing under your Stripe Services Agreement and this DPA, including international, federal, state, provincial and local Law relating to privacy, data protection or data security.

"Data Controller" means the entity which, alone or jointly with others, determines the purposes and means of Processing Personal Data, which may include, as applicable, a "Business" as defined under the CCPA.

"Data Processor" means the entity that Processes Personal Data on behalf of the Data Controller, which may include, as applicable, a "Service Provider" as defined under the CCPA.

"Data Security Measures" means technical and organizational measures that are intended to secure Personal Data to a level of security appropriate for the risk of the Processing.

"Data Subject" means an identified or identifiable natural person to which Personal Data relates.

"EEA" means the European Economic Area.

"EEA SCCs" mean Module 2 (Transfer: Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR.

"GDPR" means the General Data Protection Regulation (EU) 2016/679.

"Instructions" means this DPA and any further written agreement or documentation under which the Data Controller instructs a Data Processor to perform specific Processing of Personal Data for that Data Controller.

"Joint Controller" means a Data Controller that jointly determines the purposes and means of Processing Personal Data with one or more Data Controllers.

"Personal Data" means any information relating to an identified or identifiable natural person that is Processed in connection with the Services, and includes "personal data" as defined under the GDPR and "personal information" as defined under the CCPA.

"Process" means to perform any operation or set of operations on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, as described under DP Law.

"Sensitive Data" means (a) Personal Data that is genetic data, biometric data, data concerning health, a natural person's sex life or sexual orientation; or (b) data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, to the extent this data is treated distinctly as a special category of Personal Data under DP Law.

"SSA Affiliate" means an Affiliate of Stripe that acts as (a) a Joint Controller with Stripe in relation to Authorized Services; or (b) a Data Processor on behalf of Stripe in relation to Services other than Authorized Services.

"Sub-processor" means an entity a Data Processor engages to Process Personal Data on that Data Processor's behalf in connection with the Services.

"UK Data Transfer Addendum" means the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner's Office.

"UK GDPR" means the GDPR, as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications

(Amendments etc.) (EU Exit) Regulations 2019.

3. Stripe as Data Processor and Data Controller.

3.1. Data Processing Roles.

To the extent Stripe Processes Personal Data as a:

(a) Data Processor, it is acting as a Data Processor on behalf of you, the Data Controller; and

(b) Data Controller, it has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through you.

3.2. Categories of Data Subjects and Personal Data.

(a) *Data Subjects*. Stripe may Process the Personal Data of your Customers, representatives and any natural persons who access or use your Stripe Account.

(b) *Personal Data*. Where applicable, Stripe may Process Payment Account Details, bank account details, billing/shipping address, name, date/time/amount of transaction, device ID, email address, IP address/location, order ID, payment card details, tax ID/status, unique customer identifier, identity information including government issued documents (e.g., national IDs, driver's licenses and passports).

(c) *Sensitive Data*. Where applicable, Stripe may Process facial recognition data.

3.3. Data Processing Purposes.

(a) The purposes of Stripe's Processing of Personal Data are when Stripe is operating in its capacity as a Data Processor for a Service, including:

(i) servicing the Stripe platform; and

(ii) facilitating payment transactions on behalf of Stripe users.

(b) The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller are:

(i) determining the Processing of Personal Data when providing Stripe products and services, including when Stripe provides a payment method, and determining the third parties (banks and payment method providers) to be utilized;

(ii) monitoring, preventing and detecting fraudulent transactions and other fraudulent activity on the Stripe platform;

(iii) complying with Law, including applicable anti-money laundering screening and know-your-customer obligations; and

(iv) analyzing and developing Stripe's services.

4. Stripe Obligations when Acting as a Data Processor.

4.1. Obligations.

To the extent that Stripe is acting as a Data Processor for you, Stripe will:

(a) Process Personal Data on behalf of and according to your Instructions. Stripe will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and to comply with Law, unless otherwise permitted by your **Stripe Services Agreement** (including this DPA) or DP Law. Stripe will inform you if, in its opinion, Instructions violate or infringe DP Law;

(b) ensure that all persons Stripe authorizes to Process Personal Data in the context of the Services are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of Personal Data;

(c) to the extent required by DP Law, inform you of requests Stripe receives from Data Subjects (including "verifiable consumer requests" as defined under the CCPA) exercising their applicable rights under DP Law to (i) access (e.g., right to know under the CCPA) their Personal Data; (ii) have their Personal Data corrected or erased; (iii) restrict or object to Stripe's Processing; or (iv) data portability. Other than to request further information, identify the Data Subject, and, if applicable, direct the Data Subject to you as Data Controller, Stripe will not respond to these requests unless you instruct Stripe in writing to do so;

(d) to the extent required by DP Law, inform you of each law enforcement request Stripe receives from a Governmental Authority requiring Stripe to disclose Personal Data or participate in an investigation involving Personal Data;

(e) to the extent required by DP Law, provide you with reasonable assistance through appropriate technical and organizational measures, at your expense, to assist you in complying with your obligations under DP Law, which assistance may include conducting data protection impact assessments and consulting with a supervisory authority, taking into account the nature of the Processing and the information available to Stripe;

(f) implement and maintain a written information security program with the Data Security Measures stated in Exhibit 1 of this DPA. In addition, Stripe will implement a data security incident management program that addresses how Stripe will manage a data security incident involving the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to, Personal Data ("**Incident**"). If Stripe is required by DP Law to notify you of an Incident, then Stripe will notify you without unreasonable delay, but in no event later than any time period required by DP Law. In addition, for Incidents affecting Personal Data subject to GDPR or UK GDPR, Stripe will notify you no later than 48 hours after Stripe becomes aware of the Incident. Stripe will partner with you to respond to the Incident. The response may include identifying key partners, investigating the Incident, providing regular updates, and discussing notice obligations. Except as required by DP Law, Stripe will not notify your affected Data Subjects about an Incident without first consulting you;

(g) engage Sub-processors as necessary to perform the Services on the basis of the general written authorization you give to Stripe under Section 4.2 of this DPA;

(h) to the extent required by DP Law and upon your written request, contribute to audits or inspections by making audit reports available to you, which reports are Stripe's confidential information. Upon your written request, and no more frequently than once annually, Stripe will promptly provide documentation or complete a written data security questionnaire of reasonable scope and duration regarding Stripe's and its Affiliates' Processing of Personal Data. All documentation provided, including any response to a security questionnaire, is Stripe's confidential information; and

(i) at your choice, and subject to Stripe's rights and obligations under your **Stripe Services Agreement** (including this DPA), delete or return all Personal Data to you after the Term, and delete existing copies held by Stripe, unless Stripe is required or authorized by DP Law to store Personal Data for a longer period.

4.2 Sub-processors.

(a) You specifically authorize Stripe to engage its Sub-processors and Affiliates from the agreed lists of Sub-processors and Affiliates at stripe.com/service-providers/legal ("**Stripe Service Providers List**"). If you subscribe to email notifications at the Stripe Service Providers List, then Stripe will notify you via email of any changes Stripe intends to make to the Stripe Service Providers List at least 30 days before the changes take effect. You may reasonably object to a change on legitimate grounds within 30 days after you receive notice of the change. You acknowledge that Stripe's Sub-processors are essential to provide the Services and that if you object to Stripe's use of a Sub-processor, then notwithstanding anything to the contrary in your **Stripe Services Agreement** (including this DPA), Stripe will not be obligated to provide you the Services for which Stripe uses that Sub-processor.

(b) Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including implementing appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to you for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA.

4.3 CCPA Certification.

Where CCPA is applicable to the Services and Stripe is acting as a Data Processor, Stripe will not: (i) share (as defined by CCPA) Personal Data; (ii) retain, use or disclose Personal Data outside of its direct business relationship with User other than to provide the Stripe services and as required to comply with Law; and (iii) combine Personal Data received in connection with the Services with Personal Data received from or on behalf of an individual or collected from Stripe's own interactions with the individual except to provide the Services and as permitted by Law. Stripe certifies that it understands and will comply with the requirements in this DPA relating to CCPA and will provide the same level of privacy protection to Personal Data as required by CCPA. Stripe will inform User if it determines that it can no longer meet its obligations under CCPA and will take reasonable and appropriate steps to remediate any unauthorised Processing of Personal Data.

4.4 Disclaimer of Liability.

Notwithstanding anything to the contrary in your Stripe Services Agreement or this DPA, Stripe and its Affiliates will not be liable for any claim made by a Data Subject arising from or related to Stripe's or any of its Affiliates' acts or omissions, to the extent that Stripe was acting in accordance with your Instructions.

5. Your obligations when acting as a Data Controller.

You must:

5.1 only provide Instructions to Stripe that are lawful;

5.2 comply with and perform your obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure you have an appropriate legal basis for the Processing of Personal Data as described in your Stripe Services Agreement, including this DPA; and

5.3 provide Data Subjects with all necessary information (including by means of offering a transparent and easily accessible public privacy notice) regarding, respectively, Stripe's and your Processing of Personal Data for the purposes described in your Stripe Services Agreement, including this DPA.

6. Data transfers.

6.1 General.

Stripe and its Affiliates may transfer Personal Data on a global basis as necessary to provide the Services. In particular, Stripe and its Affiliates may transfer Personal Data to SINC in the United States and to Stripe's Affiliates and Sub-processors in other jurisdictions. Where Stripe transfers Personal Data under this DPA to a country or recipient not recognised as having an adequate level of protection for Personal Data according to DP Law, Stripe will comply with its obligations under DP Law.

6.2 Transfers from the EEA to SINC.

The EEA SCCs apply to a transfer from the EEA of Personal Data Processed under this DPA between you and SINC and are incorporated into this DPA. You agree that the EEA SCCs are completed and supplemented as follows:

(a) you are the data exporter and SINC is the data importer;

(b) the optional docking clause under Clause 7 of the EEA SCCs will not apply;

(c) option 2 under Clause 9 of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to Section 4.2 of this DPA;

(d) the optional redress language under Clause 11(a) of the EEA SCCs will not apply;

(e) the governing law under Clause 17 of the EEA SCCs will be Ireland;

(f) the choice of forum and jurisdiction under Clause 18 of the EEA SCCs will be the courts of Ireland;

(g) Annexes I, II and III of the EEA SCCs are deemed to be populated with the information set out in Exhibits 1 and 2 of this DPA; and

(h) Annex IV of Exhibit 2 of this DPA supplements the EEA SCCs with additional clauses.

6.3 2010 SCCs.

For the purposes of a transfer of Personal Data from the EEA, Switzerland or the United Kingdom, any reference to the standard contractual clauses adopted under Directive 95/46/EC ("**2010 SCCs**") in an agreement you have entered into with Stripe or its Affiliates will be construed as a reference to the Approved Data Transfer Mechanism. The 2010 SCCs are terminated and replaced by the Approved Data Transfer Mechanism. Any Personal Data transferred under the 2010 SCCs will not be returned or destroyed due to the termination of the 2010 SCCs and instead will become subject to the Approved Data Transfer Mechanism.

6.4 Transfers from the United Kingdom to SINC.

The UK Data Transfer Addendum applies to a transfer from the United Kingdom of Personal Data Processed under this DPA between you and SINC and is incorporated into this DPA. You agree that the UK Data Transfer Addendum is completed and supplemented as follows:

(a) you are the data exporter and SINC is the data importer;

(b) Table 1 of the UK Data Transfer Addendum is deemed to be populated with the information set out in Annex IA of Exhibit 2 of this DPA;

(c) for the purposes of Table 2 of the UK Data Transfer Addendum, the version of the "Approved EU SCCs" (including the appendix information, modules and selected clauses) appended to the UK Data Transfer Addendum is the EEA SCCs:

(d) the optional docking clause under Clause 7 of the EEA SCCs will not apply;

(e) option 2 under Clause 9 of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to Section 4.2 of this DPA;

(f) the optional redress language under Clause 11(a) of the EEA SCCs will not apply;

(g) Annex IV of Exhibit 2 of this DPA supplements the EEA SCCs with additional clauses;

(h) Table 3 of the UK Data Transfer Addendum is deemed to be populated with the information set out in Exhibits 1 and 2 of this DPA;

(i) the "importer" and "exporter" option applies for the purposes of Table 4 of the UK Data Transfer Addendum;

(j) under Part 2, the mandatory clauses of the UK Data Transfer Addendum will apply; and

(k) by using the Services to transfer Personal Data to SINC, you will be deemed to have signed the UK Data Transfer Addendum.

6.5 Transfers from other countries or regions.

The terms applicable to the transfer of Personal Data processed under this DPA from any country or territory listed in Exhibit 3 of this DPA, including any Approved Data Transfer Mechanism, are incorporated into this DPA.

7. Conflict.

If there is any conflict or ambiguity between:

7.1 the provisions of this DPA and the provisions of your **Stripe Services Agreement** regarding Personal Data Processing, the provisions of this DPA will prevail; and

7.2 the provisions of this DPA and any provision contained in an Approved Data Transfer Mechanism and executed by you and SINC, the provisions of the Approved Data Transfer Mechanism will prevail.

EXHIBIT 1: STRIPE DATA SECURITY

1. Security Programs and Policies

1.1. Stripe maintains and enforces a security program that addresses how Stripe manages security, including the security controls Stripe employs. The security program includes:

(a) documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;

(b) documented, clear assignment of responsibility and authority for security program activities;

(c) policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media and remote access; and

(d) regular testing of the key controls, systems and procedures.

1.2. Privacy Program.

Stripe maintains and enforces a privacy program and related policies that address how Personal Data is collected, used and shared.

2. Risk and Asset Management

2.1. Stripe performs risk assessments, and implements and maintains controls for risk identification, analysis, monitoring, reporting and corrective action.

2.2. Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.

3. Personnel Education and Controls

3.1. All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively "**Personnel**") acknowledge their data security and privacy responsibilities under Stripe's policies.

3.2. For Personnel, Stripe, either itself or through a third party:

(a) implements pre-employment background checks and screening;

(b) conducts security and privacy training;

(c) implements disciplinary processes for violations of data security or privacy requirements; and

(d) upon termination or applicable role change, promptly removes or updates Worker access rights and requires the Worker to return or destroy Personal Data.

3.3. Authentication.

Stripe authenticates each Personnel's identity through appropriate authentication credentials such as strong passwords, token devices or biometrics.

4. Training and Awareness

Annual Security and Privacy Training. Stripe's employees complete an annual Security and Privacy awareness training on Stripe's data security and confidentiality policies and practices.

5. Network and Operations Management

5.1. Policies and Procedures.

Stripe implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation.

5.2. Vulnerability Assessments.

Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data.

6. Technical Access Controls

6.1. Access control.

Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:

(a) user identification and authentication procedures;

(b) ID/password security procedures (special characters, minimum length, change of password), including stronger digital authentication measures based on NIST 800-63B;

(c) automatic blocking (e.g., password or timeout); and

(d) break-in-attempt monitoring.

6.2. Data access control.

Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to the Personal Data allowed for their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

(a) internal policies and procedures;

(b) control authorization schemes;

(c) differentiated access rights (profiles, roles, actions and objects);

(d) access monitoring and logging;

(e) access reports;

(f) access procedure;

(g) change procedure; and

(h) deletion procedure.

7. Physical access controls

7.1. Stripe uses reputable third-party service providers to host its production infrastructure. Stripe relies on these third parties to manage the physical access controls to the data center facilities that they manage. Some of the measures that Stripe's service providers provide to prevent unauthorized persons from gaining physical access to the data processing systems available at premises and facilities (including databases, application servers and related hardware), where Personal Data is Processed, include:

(a) physical access control system and program in place at Stripe premises;

(b) 24x7 Global Security Operation Center that monitors physical security systems;

(c) security video and alarm systems;

(d) access control roles and area zones;

(e) access control audit measures;

(f) electronic tracking and management program for keys;

(g) access authorisations process for employees and third parties;

(h) door locking (electrified locks etc.); and

(i) trained uniformed security staff.

7.2. Stripe reviews third-party audit reports to verify that Stripe's service providers maintain appropriate physical access controls for the managed data centers.

8. Availability Controls

Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:

8.1. database replication;

8.2. backup procedures;

8.3. hardware redundancy; and

8.4. a disaster recovery plan.

9. Disclosure Controls

Stripe implements measures to ensure that Personal Data (a) cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic); and (b) can be verified to which companies or other legal entities Personal Data are disclosed, including logging, transport security and encryption.

10. Entry Controls

Stripe implements measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including logging and reporting systems, and audit trails and documentation.

11. Separation Controls

Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including:

11.1. "least privilege" limitation of access to data by internal service;

11.2. segregation of functions (production/testing);

11.3. procedures for storage, amendment, deletion, transmission of data for different purposes; and

11.4. logical segmentation processes to manage the separation of Personal Data.

12. Certifications and Reports

12.1. PCI Compliance.

To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS requirements. Stripe's PCI certification is confirmed annually by a qualified security assessor (QSA).

12.2. SOC Reports.

Stripe maintains Service Organization Controls ("**SOC**") auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided upon request.

12.3. Stripe may add standards or certifications at any time.

13. Encryption

13.1. Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit. Access to Stripe cryptographic key materials is restricted to a limited number of authorized Stripe personnel.

13.2. Encryption in transit.

To protect data in transit, Stripe requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol. For data traversing Stripe's internal production networks, Stripe uses mTLS to encrypt connections between production systems.

13.3. Encryption at rest.

To protect data at rest, Stripe uses industry standard encryption (AES 256) to encrypt all production data stored in server infrastructure.

13.4. Payment Card and Banking Account Data Tokenization.

Payment card and bank numbers are separately encrypted using industry standard encryption (AES-256) at the data level and stored in a separate data vault that is highly restricted. Decryption keys are stored on separate machines. Tokens are generated to support Stripe data processing.

14. Data Security Incident Management and Notification

14.1. Stripe implements a data security incident management program that addresses how Stripe manages Incidents.

14.2. Stripe will notify impacted Stripe users and Governmental Authorities (where applicable) of Incidents in a timely manner as required by DP Law.

15. Reviews, Audit Reports and Security Questionnaires

Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data technology environment in relation to the Processing of Personal Data. Stripe's responses to the security questionnaire are Stripe's confidential data.

16. System Configuration

16.1. Stripe implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance.

16.2. Stripe relies on deployment automation tools to deploy infrastructure and system configuration. These automation tools leverage infrastructure configurations that are managed through code that flows through Stripe's change control processes. Stripe's change management processes require formal code reviews and two-party approvals prior to the release to production.

16.3. Stripe uses monitoring tools to monitor production infrastructure for changes from known configuration baselines.

17. Data Portability

The Stripe API enables Stripe users to programmatically access the data stored for transfer, excluding PCI-scoped data. The portability process for PCI data to other PCI-DSS Level 1 compliant payment processors can be found at https://stripe.com/docs/security/data-migrations/exports.

18. Data Retention and Deletion

Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate.

EXHIBIT 2: APPROVED DATA TRANSFER MECHANISM: DESCRIPTION OF PROCESSING AND TRANSFER

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The party to the Stripe Services Agreement with Stripe or its Affiliate (as applicable).

Address: The data exporter's address.

Contact person's name, position and contact details: The name, position and contact details provided by the data exporter.

Activities relevant to the data transferred under these Clauses: Processing Personal Data in connection with the data exporter's use of the Services under the Stripe Services Agreement.

Role (controller/processor): Controller

Signature and date: By using the Services to transfer Personal Data to the data importer, the data exporter will be deemed to have signed this Annex I.

Data importer:

Name: Stripe, Inc.

Registered office: Corporation Trust Center, 1209 Orange Street, Wilmington, New Castle, DE 19801, USA

Contact details: Stripe Privacy Team, privacy@stripe.com

Activities relevant to the data transferred under these Clauses: Processing Personal Data in connection with the data exporter's use of the Services under the Stripe Services Agreement.

Role (controller/processor): Processor

Signature and date: The data importer will be deemed to have signed this Annex I on the transfer of Personal Data by the data exporter in connection with the Services.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The Personal Data transferred concern the following categories of Data Subjects or consumers:

Users of the data importer's online and mobile services.

The data exporter's end customers, donors, representatives and any natural person who accesses or uses your Stripe Account.

Categories of personal data transferred

The categories of Personal Data transferred are described in Section 3 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The categories of Personal Data transferred are described in Section 3 of the DPA.

The frequency of the transfer (whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer is a continuous basis for the duration of the **Stripe Services Agreement** until the Personal Data is deleted in accordance with Section 4.1(i) of the DPA.

Nature of the processing

The nature of the processing is described in Section 3 of the DPA.

Purpose(s) of the data transfer and further processing

The purposes of the data transfer are described in Section 3 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained is set out in Section 4.1(i) of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter and nature of the processing related to transfers to Sub-processors is set out at Annex III to these clauses. Subject to Section 4.1(i) of the DPA, the duration of the processing is the duration of the **Stripe Services Agreement**.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of the EEA SCCs is the Irish Data Protection Commission.

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The data importer will maintain and implement the technical and organizational measures set out in Exhibit 1 of the DPA.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has generally authorized the engagement of the Sub-processors at https://stripe.com/service-providers/legal.

ANNEX IV

SUPPLEMENTAL CLAUSES

In addition to the obligations under the EEA SCCs and the UK Data Transfer Addendum (as applicable), the parties agree to the following supplementary measures:

1.Personal Data will be encrypted both in transit and at rest using encryption technology by the data importer.

2.the data importer will resist, to the extent permitted by Law, any request under Section 702 of Foreign Intelligence Surveillance Act ("**FISA**").

3.the data importer will use reasonably available legal mechanisms to challenge any demands for data access through the national security process that it may receive in relation to data exporter's data.

4.no later than the date on which the data exporter's acceptance of the DPA and the Approved Data Transfer Mechanism that incorporates or references this Annex becomes effective, the data importer will notify the data exporter of any binding legal demand for the Personal Data it has received, including national security orders and directives, which will encompass any process issued under Section 702 of FISA, unless prohibited under Law.

5.the data importer will ensure that Stripe's data protection officer has oversight of Stripe's approach to international data transfers.

This Annex also sets out the parties' interpretation of their respective obligations under the specific terms of the EEA SCCs (as amended or supplemented by an Approved Data Transfer Mechanism). Where a party complies with the interpretations set out in this Annex, that party will be deemed by the other party to have complied with its commitments under the EEA SCCs.

6.**Clause 8.1(a): Instructions**
The DPA and the **Stripe Services Agreement** are the data exporter's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing by the parties. For the purposes of Clause 8.1(a) of the EEA SCCs, the Processing described in the DPA is deemed an instruction by the data exporter to Process Personal Data.

7.**Clause 9(c): Copies of Sub-processor Agreements**
The parties agree that, following a request by the data exporter, the data importer will provide copies of the Sub-processor agreements that must be provided to the data exporter pursuant to Clause 9(c) of the EEA SCCs, provided that

the data importer may (i) redact or remove all commercial information, or clauses unrelated to the EEA SCCs or their equivalent and (ii) determine the manner in which to provide the copy agreements to the data exporter.

8.**Clause 8.9(k) and (l): Audit**
The data exporter acknowledges and agrees that it exercises its audit right under Clause 8.9(k) and (l) of the EEA SCCs by instructing the data importer to comply with the audit measures described in Section 4.1(h) of the DPA.

9.**Additional commercial clause**
The EEA SCCs are incorporated into the **Stripe Services Agreement**. As between the data exporter, and the data importer and its Affiliates, to the greatest extent permitted by Law, the limitations and exclusions of liability set out in the Stripe Services Agreement will apply to the EEA SCCs.

10.**Defined terms**
Capitalized terms not defined in these Annexes have the meanings given to them in the **Stripe Services Agreement**, including the DPA.

EXHIBIT 3: JURISDICTION SPECIFIC TERMS AND APPROVED DATA TRANSFER MECHANISMS

SWITZERLAND

The EEA SCCs in the form described in Section 6.2 of the DPA and as adapted and supplemented as described in this Exhibit 3, will only apply to a transfer of Personal Data Processed under this DPA from Switzerland to SINC. For these purposes, you agree that:

1. any reference to “Member State” will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);
2. any references to “personal data” extend to personal data of legal entities if and to the extent such personal data pertaining to legal entities is within the scope of the Swiss Federal Act on Data Protection ("**FADP**"); and
3. to the extent the transfer of personal data is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority; to the extent the transfer of personal data is governed by the GDPR, the supervisory authority determined in Annex IC will act as the competent supervisory authority; any references to the "competent supervisory authority" will be interpreted accordingly.

Download the DPA

Click here to download the Stripe DPA

Stripe Services Agreement
Stripe Connected Account Agreement
Stripe Payments Company Terms
Acquirer Terms
- Cross River Bank
- PNC Bank

stripe

Stripe Privacy Center

Last updated: May 17, 2023

Welcome to the Stripe Privacy Center

Stripe respects the privacy of everyone that engages with our platform, and we are committed to being transparent about our privacy processes and policies. We are a platform that enables millions of businesses, and in order to provide our services to our Business Users and End Users, we collect and process personal data.

The Stripe Privacy Center contains the answers to frequently asked questions about how we collect and use personal data, the rights that individuals have in relation to personal data held by Stripe, and how Stripe complies with international data protection laws.

All materials have been prepared for general information purposes only. The information presented is not legal advice, is not to be acted on as such, may not be current and is subject to change without notice.

Stripe's updated Privacy Policy will be effective as of January 24, 2023

We're updating our Privacy Policy to clearly explain how we collect and use data as we work to improve the Stripe experience.

Here's a summary of key changes:

- We added more clarity about how our services use Personal Data.
- We clarified how we will use Personal Data for Stripe's own marketing purposes to Visitors, End Users and Representatives.
- We updated the information on our legal bases for cross-border data transfers, including those between the EEA and US.
- We added more information about privacy rights that exist in some countries where Stripe offers services.

These are just a few highlights of the changes we made, so please read the updated Privacy Policy below carefully. If you have questions, please check out the rest of our Privacy Center and/or contact us.

Below is a list of terms that will help "you" navigate the Privacy Center:

"YOU"	MEANING	STRIPE EXAMPLES
Business User	Stripe provides services to entities ("Business Users") who directly and indirectly provide us with "End Customer" Personal Data in connection with those Business Users' own business and activities.	Stripe user or merchant Platform User Connect Accounts
End Customer	When you do business with, or otherwise transact with, a Business User (typically a merchant using Stripe Checkout, e.g. when you buy a pair of shoes from a merchant that uses Stripe for payment processing) but are not directly doing business with Stripe, we refer to you as an "End Customer."	Individual using Identity Cardholder using Checkout
End User	When you directly use an End User Service (such as when you sign up for Link, or make a payment to Stripe Climate in your personal capacity), for your personal use, we refer to you as an "End User."	User of Link Personal contributor to Stripe Climate
Representative	When you are acting on behalf of an existing or potential Business User (e.g. you are a founder of a company, or administering an account for a merchant who is a Business User), we refer to you as a "Representative."	Beneficial owner Shareholder, officer, director Account representative
Visitor	When you visit a Site without being logged into a Stripe account or otherwise communicate with Stripe, we refer to you as a "Visitor." (e.g. you send Stripe a message asking for more information because you are considering being a user of our products).	Stripe Sessions attendee Stripe Site visitor

Contents

How We Collect, Disclose, and Use Personal Data

Is Stripe acting as a data controller or a data processor?

The answer is both.

The “data controller” is the entity which determines the purposes and means of the data processing taking place. The “data processor” is an entity acting on behalf and under the instructions of a controller in processing personal data.

Stripe is a data controller when it determines the purposes and means of the processing taking place. These data processing activities include (1) providing the Stripe products and services, (2) monitoring, preventing and detecting fraudulent payment transactions and other fraudulent activity on the Stripe platform, (3) complying with legal or regulatory obligations applicable to the financial sector to which Stripe is subject, and (4) analyzing, developing and improving Stripe’s products and services. Please see this Privacy Center article for more information on Stripe’s controller activities.

Stripe is a data processor where it is facilitating payment transactions on behalf of and at the direction of a Business User. Our Business Users direct us to take payment from cardholders / End Customers.

Stripe is considered a processor when directed to process payments (i.e., Stripe receives instructions about whom to pay, how much to pay, when to pay).

As a platform provider, we need to ensure consistency across our platform, and that includes consistency with respect to the commitments that we give about how we operate our platform. We contract with all of our Business Users (including some of the world’s largest companies) on this basis.

Which Stripe entities are involved?

For most of our services, it is either Stripe, Inc., the US parent company operating under US law, or Stripe Payments Europe, Limited (“SPEL”), an Irish company operating under Irish law, the data controller responsible for Personal Data collected and processed in relation to Stripe Services.

The Stripe entity responsible for your data will depend on your location, the product or service you use with us and whether Stripe is acting as a controller and/or data processor.

If you are located outside of the Americas (e.g., European Economic Area ("EEA"), Switzerland or the United Kingdom, countries located in Asia Pacific ("APAC")), SPEL is the primary entity responsible for the processing of your personal data. Some of the payment processing services offered by Stripe are services that may be only provided for by an authorised payment services provider or electronic money institution. In this case, SPEL and the Stripe local regulated entity (defined as those who are licensed, authorized or registered by a Local Regulatory Authority) will act as joint controllers of your Personal Data.

Please see our table below for more information on who is your controller in these jurisdictions:

LOCATION OF USER	PURPOSE OF PROCESSING	NAME OF STRIPE ENTITY	LOCATION OF STRIPE ENTITY
EEA	Provision of certain authorised payment services in the EEA and Switzerland Please see https://stripe.com/ie/ssa	Stripe Technology Europe, Limited (the e-money licensed entity with the Central Bank of Ireland)	Ireland
EEA	All other activities.	SPEL	Ireland
United Kingdom & Switzerland	Provision of authorised payment services in the UK. Please see https://stripe.com/gb/ssa	Stripe Payments UK, Ltd. (the e-money licensed entity with the UK FCA)	United Kingdom
United Kingdom & Switzerland	All other activities.	SPEL	Ireland
United Kingdom	Provision Stripe Capital product and related services to Stripe users in the UK.	Stripe Capital Europe, Limited	Ireland

Stripe affiliates also provide local support services in certain countries where Stripe operates. These entities act as data processors on behalf of Stripe, Inc. or SPEL, depending on the jurisdiction. You will find the most up-to-date list of the Stripe affiliates on this page.

For certain products, Stripe may act as an independent controller (e.g. Stripe Capital), a data processor or both (e.g. Stripe Identity). Please see the Privacy Center article for each specific product for more information.

What are your data controller activities?

Providing the Stripe products and services to Business Users and End Users, including determining the third parties (banks and payment method providers) to be utilized;

Monitoring, preventing and detecting fraudulent payment transactions and other fraudulent activity on the Stripe platform;

Complying with legal or regulatory obligations applicable to the financial sector to which Stripe is subject, including applicable anti-money laundering screening and compliance with know-your-customer obligations; and

Analyzing, developing and improving Stripe's products and services.

How does Stripe use personal data to improve its products and services?

Stripe collects data, including personal data, while providing services to its users. Stripe uses some of the data it collects to improve its products and services, including by training the models it employs for fraud and loss prevention and to analyze the performance of Stripe's products as permitted by applicable law and agreements.

Personal data is required to train Stripe's fraud and loss prevention models, including those employed by Stripe Radar and Stripe Identity. These products rely in part on their ability to recognize certain characteristics that help determine whether a transaction is fraudulent or unlikely to complete. For example, they compare Personal Data presented in a specific transaction to Personal Data collected in the past to identify when a fraudster is attempting to perpetrate fraud, including to impersonate a Stripe User or their End Customers.

In addition to using Personal Data to train its fraud and loss prevention models, Stripe also uses transaction data to assess the functioning of its current products and proposed product improvements. For instance, Stripe uses data collected by its java script library stripe.js to assess the performance of the checkout surfaces it provides to Business Users, and payment authorization data to evaluate ways to improve authorization rates for Business Users. Stripe uses Personal Data, such as IP address, to identify which pages and features a user interacted with during a checkout session, so that it can assess the effect different features have on the outcome of a checkout session.

Stripe uses pseudonymized or aggregated transaction data for these purposes in certain circumstances. When Stripe communicates the results of its product performance analytics to Business Users or for advertising purposes, it does so only in aggregated or de-identified form that does not permit third-parties outside of Stripe to associate that data with any particular End Customers.

You should consult your legal counsel regarding how best to disclose Stripe's data usage to your customers. But, here is a paragraph you could add to your privacy policy if it doesn't already include such a disclosure:

> We use Stripe for payments, analytics, and other business services. Stripe may collect personal data including via cookies and similar technologies. The personal data Stripe collects may include transactional data and identifying information about devices that connect to its services. Stripe uses this information to operate and improve the services it provides to us, including for fraud detection, loss prevention, authentication, and analytics related to the performance of its services. You can learn more about Stripe and read its privacy policy at **https://stripe.com/privacy**.

As a Stripe User and as a data controller, what does GDPR mean for me?

As a data controller, Business Users are responsible for the relationship with the data subject (i.e., your End Customer). You may instruct a third party (like Stripe) to process the data, but it is your job to set the purpose (or objectives) and legal basis for the processing.

The GDPR requires data controllers to use third parties who agree to abide by certain contractual terms. To be sure of this, the data controller must have Data Processing Agreements ("DPAs") with each third party. Our DPA has been designed to serve this purpose for you; it is strongly aligned with payment transactions, so it should establish that you are compliant with GDPR from a payments perspective.

Who are Stripe's sub-processors and how are they vetted?

Please see our service providers page where we have a list of our most common sub-processors, service providers and affiliates. Stripe identifies, evaluates, and engages sub-processors through our vendor management program. We enter into a contract with each sub-processor prior to sharing data with the sub-processor, and each contract contains terms that provide for monitoring and audit. In addition, all potential vendors are vetted and approved through Stripe's security review process before we begin using their services.

From where does Stripe collect information used for fraud prevention and security purposes?

To prevent fraud and strengthen our security, we may collect information from Business Users, End Customers, End Users, financial parties, and in some cases third parties. For example, we collect and analyze information that helps us identify bad actors and bots, including both transactional data (such as amount, customer shipping address, date, and so on) and advanced fraud detection signals (device and activity signals). Learn more.

Stripe also receives information from third parties to prevent and respond to security incidents, and for protecting against other fraudulent activity. For example, we may receive information from third parties about IP addresses that malicious actors have compromised. Stripe may use Representatives' Personal Data provided at onboarding to query third party databases regarding fraud and risk signals associated with that data. The third party providers operating these databases may use Stripe's experience with the Personal Data queried to inform their fraud and risk signals.

How does Stripe use Personal Data to prevent fraud?

The Stripe products that use Personal Data to enable Stripe's Business Users to detect and prevent fraud include Stripe Radar and Stripe Identity. Stripe also employs internal risk models and other product features, such as 3D Secure incorporated into Stripe's Issuing product, to prevent its products and services from being used for fraudulent activity.

Stripe Radar processes personal data as described here using its machine learning model to produce scores indicating the likelihood that a payment method is being offered by someone other than an authorized user. These scores are designed to identify fraudulent transactions, they do not rate the character or creditworthiness of the individuals involved in a particular transaction. Based on the service selected by the Business User, Stripe may provide the Radar scores to its Business Users to help them to combat fraud and provide a mechanism for them to set rules to better manage transactions based on Radar scores and other indicators of fraud.

Stripe Identity uses Personal Data, as described here, to combat fraud by enabling Business Users to verify whether the person they are transacting with is who they say they are. Identity compares biometric identifiers in a selfie against government issued ID. Identity can also validate Personal Data, such as name, date of birth, and government ID number, that an End Customer types into a web form against government and third-party databases to determine if the identity presented matches the government issued ID number.

Stripe's internal risk models seek to combat fraud by recognizing when a fraudster is attempting to use Stripe's services for fraudulent purposes. For instance, Stripe uses Radar scores internally to determine whether a payment method offered to Stripe products such as Link, Frontier, Crypto Onramp, and Bill Pay should be accepted or rejected as likely fraudulent. Stripe's internal risk models also use aggregated cardholder features to recognize when a large number of transactions are likely being conducted by the same individual for purposes of testing or cashing out stolen payment methods. Where Stripe recognizes such activity, it will block transactions to prevent harm to itself, its users, and others.

Along with attempting to combat fraud at the merchant and Stripe-wide levels as described above, Stripe also incorporates features in its individual products that use Personal Data to prevent fraud. One such feature is 3D Secure authentication, incorporated in Stripe Issuing. This feature is required by law in certain jurisdictions and requires cardholders to authenticate using one or more factors before they can complete an online transaction. Stripe and its service providers use and store personal data including cardholder PANs, contact information, and transaction history to authenticate cardholders using one time passcodes and knowledge of past transactions. These measures help combat fraud by increasing the likelihood that the person offering a card for payment is an authorized user.

I heard that Stripe is collecting additional information about my account from a third party and/or my other Stripe account. Why is Stripe collecting this information?

Stripe may collect additional information about your account to allow Stripe and its financial partners to detect fraud and/or fulfill financial compliance requirements. These requirements come from our financial partners or regulatory obligations and are intended to prevent abuse of the financial system. Examples of missing data fields include your address, phone number, social security number, date of birth, employer identification number, or website URL. Stripe may be able to fill in some of this information by leveraging data we have collected from one of your other Stripe accounts or by obtaining data from a third party. We will show Business Users the information that we are associating with their account on your dashboard, and Business Users may update or correct that information via your dashboard. Please see Stripe's Privacy Policy for additional information.

Does Stripe collect precise location data?

Devices such as mobile phones or computers may collect precise location data using GPS technology. Stripe does not collect GPS data from devices and browsers.

Depending on the Services you use and the Business Users' implementation of our Business Services, we will collect information (including IP addresses) through cookies and similar technology. We will collect your IP address when you visit our Sites. Please see our Cookie Policy to learn more. Stripe may use location information, including approximate latitude and longitude, derived from End Customers IP addresses to detect potentially fraudulent transactions.

We also receive approximate location information (such as country, city or state) from third party providers such as MaxMind to help us determine the approximate location of visitors to our website for marketing purposes (for example, inviting you to local Stripe events).

Does Stripe sell my personal information under the CCPA?

Stripe does not sell personal information. As such, Stripe does not sell personal information of minors under 16 years of age. For California residents, the California Consumer Privacy Act ("CCPA") defines "selling" personal information to include providing it to a third party in exchange for money or valuable consideration.

What data does Stripe disclose to third parties and for what purposes?

For Shine the Light law (Cal. Civ Code § 1798.83) purposes, Stripe does not share personal data of California customers to third parties for their direct marketing purposes, as defined by this law.

The table below discloses the categories of personal information about California consumers that we collect and disclose for a business purpose.

CATEGORIES OF PERSONAL INFORMATION COLLECTED	DISCLOSED FOR A BUSINESS PURPOSE IN THE PRECEDING 12 MONTHS	TO WHOM THE DATA MAY BE DISCLOSED
Identifiers (for example, a device identifier)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Characteristics of protected classifications under California or federal law (for example, gender and age noted in ID documents that you submit so that Stripe can verify your identity on behalf of your merchant - a.k.a. our business user)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Commercial information (for example, the merchant that you choose to do business with - a.k.a. our business user - may receive your transaction data)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Biometric information (for example, biometric identifiers from photo IDs used to confirm your identity)	Yes	We may disclose the data, pursuant to applicable law, to: a service provider - i.e., Amazon Web Services ("AWS"), an entity engaged in a business

CATEGORIES OF PERSONAL INFORMATION COLLECTED	DISCLOSED FOR A BUSINESS PURPOSE IN THE PRECEDING 12 MONTHS	TO WHOM THE DATA MAY BE DISCLOSED
		transfer/merger, law enforcement, courts, governments and regulatory agencies.
Online activity information (for example, information about devices and browsers across certain business user sites that use Stripe and IP addresses associated with those devices and browsers, and usage data)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Geolocation Data (for example, IP addresses)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Audiovisual (for example, visual, audio, or similar information, like photos you submit so that Stripe can verify your identity on behalf of your merchant – a.k.a. our business user)	Yes	We may disclose the data, pursuant to applicable law, to: service providers, the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Professional or Employment-Related Information	Yes	We may disclose the data, pursuant to applicable law, to: Service Providers, an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.
Categories of personal information described in Cal. Civ. Code 1798.80(e) (such as name, address, telephone number, credit card or debit card number)	Yes	We may disclose the data, pursuant to applicable law, to: service enablers (like service providers and financial partners servicing the financial product), the merchant that you do business with (a.k.a. our business user), an entity engaged in a business transfer/merger, law enforcement, courts, governments and regulatory agencies.

What sensitive personal information under the California Consumer Privacy Act (CCPA) does Stripe collect and for what purposes does Stripe use that

data?

Stripe only processes sensitive personal information for the purposes specified in section 7027(m) of the California Consumer Privacy Act Regulations, or without the purpose of inferring characteristics about a consumer.

Sensitive Personal Information Categories	Purposes include:
Identification card, including driver's license, passport, and social security (including any underlying sensitive information in the identity card, such as racial or ethnic origin)	Identity verification, fraud prevention and security, to provide the services, and to comply with legal obligations.
Biometric information	Identity verification, fraud prevention and security, and for other purposes consistent with your consent and applicable law, such as to improve our verification systems. Learn more.
Location data Learn more	Fraud detection and security, in furtherance of compliance with legal obligations, and to provide the services including to market our products.
Account log-in, financial account in combination with any required security access code, password, or credentials allowing access to an account	To provide you the service that you requested from your merchant (i.e., our Business User) and/or Stripe, verify your account, facilitate the processing of your requested payments, provide customer support, comply with law, enforce our terms of services, and for other purposes consistent with your consent and applicable law.

In addition to its sub-processors, what other third parties does Stripe share information with?

When we work with service providers in our capacity as a data processor for our Business Users' and End Users' personal data, the GDPR calls these third-party service providers a sub-processor. Sub-processors are service providers who have or potentially will have access to or process personal data on behalf of Stripe. These third parties are disclosed on our Stripe Service Providers List.

In addition to Stripe's sub-processors, we may also share Business Users' onboarding data and payment instrument information with third party business partners when this is necessary to provide our services to our Business Users. We do so, for example, for the purposes of offering payment processing services to our Business Users or facilitating payment settlements.

Third parties to whom we may disclose personal data for this purpose are banks, payment method providers and payment processors, including, but not limited to, the following entities:

American Express Payment Services Limited and American Express Payments Europe S.L.

Banking Circle S.A.

Barclays Bank PLC

Citibank Europe plc

Credit Mutuel Arkea and Arkea Banking Services

Currence iDEAL B.V.

Klarna AB

Mastercard Europe S.A.

Polski Standard Płatności

PPRO Financial Ltd.

Swisscard AECS GmbH

Visa Europe Limited

The data shared with payment method providers will depend on the payment method(s) enabled on the Business User's account.

In addition, Stripe shares personal data as we believe necessary to, among other things, protect Stripe's services, rights, privacy, safety and property of Stripe, our users or others. For example, to protect our services, Stripe may receive or disclose information about IP addresses that malicious actors have compromised.

Please note that if you provide us with your payment method information (e.g. a card number and expiration date) to store on file, Stripe will update your card information if your information has changed or been updated to ensure your transactions go through smoothly, including by working with your card issuer. If you would prefer to not have your updated payment method details shared with us, please reach out to your card issuing bank.

Transfer

Stripe will pass on personal data to affiliates and service providers or sub-processors, if deemed strictly necessary to carry out contractual obligations or for the data to be processed. Depending on the enabled payment method(s), data may be transferred to the jurisdiction(s) of the respective payment method(s). Before we engage any third party, we perform due diligence, including a vendor security assessment. All of our service providers are subject to contract terms designed to ensure that these service providers process personal data only for the purposes of providing services to Stripe and in accordance with our commitments to Users and applicable data protection laws. Moreover, Stripe maintains and enforces a security program that addresses the management of security and the security controls employed by Stripe, which includes third party risk management. In addition, Stripe employees, agents, and contractors acknowledge their data security and privacy responsibilities under Stripe's policies.

Financial Connections

If you are an End Customer who has been asked to link your financial account using Stripe, please visit the support webpage **here** to learn more about our privacy practices. Or you can jump to the specific topics linked here:

Linking my financial account and consent

Data collected, stored, and shared from my linked account

How Stripe accesses data from my linked account

What Business User and Representative data does Stripe share with a payment method to facilitate Business Users' enabling the payment method?

Stripe makes it possible for its Business Users to enable payment methods including card networks such as Visa and MasterCard, mobile and online payment methods such as WeChat Pay and Alipay, and buy now pay later providers such as Klarna and Afterpay. Certain payment methods are enabled by default when you onboard with Stripe and you can choose to enable additional payment methods through your Stripe dashboard. When, either during or after onboarding, a payment method is enabled on a Business User's Account, the payment method provider may require Business Users' and their Representatives' Personal Data for a number of purposes, including complying with know your customer (KYC), anti-money laundering, and other legal and compliance requirements, preventing fraud, facilitating transactions, and providing services to Business Users. For these purposes, Stripe may provide payment method providers with Business User data, including but not limited to business name, business type, merchant category codes, merchant ID, transaction history, and bank account information. Stripe may also provide payment methods with Business Users' Representatives' personal data, including name, address, contact information, date of birth, tax identification number, and other government issued ID information.

What data about End-Customers and their transactions is used by Radar and what data does Stripe share with its Radar Business Users?

When processing payments, it's valuable to Stripe, Business Users and End Customers to enable legitimate transactions while also trying to prevent fraudulent transactions, making online purchases safer for everyone involved. **Radar** helps detect potentially fraudulent transactions for Stripe's Business Users (i.e., merchants) through **machine learning** and other techniques. To do this, Radar leverages data collected across our Services.

Radar's machine learning model produces transaction "scores" indicating the model's assessment of the likelihood that a transaction is fraudulent. Business Users can leverage this score and use it to implement automated rules to determine whether to allow, block, or flag transactions for additional review. Business Users can use Radar as one of multiple inputs in making decisions with respect to the potential for fraud in a transaction.

Radar uses data collected about the End Customer from various sources, including payments transaction data, **advanced fraud detection** data, Bank Connections data, IP address, and physical address information. Radar uses this data to assess whether the payment method offered by the End Customer is likely unauthorized.

Stripe may share with the Business User and allow them to export (where allowed by Law) certain information relevant to fraud detection, including:

- a transaction score that assesses the likelihood of the transaction becoming a fraudulent charge-back,
- **risk insights** for that transaction,
- **related payments** made by the End-Customer to the Business User,
- **other transaction data** related to that End-Customer's transaction with that Business User (e.g., cardholder name, card information, and the payment amount and date),
- device and browser information for the device used to make the transaction with that Business User, and
- **aggregated benchmarks**.

As noted in Stripe's **Privacy Policy**, Stripe does not sell personal data, it provides this data to Business Users to facilitate their use of Stripe's fraud prevention services.

As a Business User, what notice do I provide to my End Customers about Stripe?

Under the terms of our agreements, Business Users are required to provide all necessary notices and obtain all necessary rights and consents from their End Customers to enable Stripe to lawfully collect, use, retain and disclose the Personal Data as part of the Stripe Services. Business Users, as data controllers, are responsible for the contents of their privacy notice and cookie banner. As an example, here is a paragraph that you can consider adding to your privacy notice (if you don't already have such a disclosure):

We use Stripe for payment, analytics, and other business services. Stripe collects and processes personal data, including identifying information about the devices that connect to its services. Stripe uses this information to operate and improve the services it provides to us, including for fraud detection and prevention. You can learn more about Stripe and its processing activities via privacy policy at https://stripe.com/privacy.

Please be aware that the disclosure above is for illustrative purposes only and is not legal advice. Please talk to your legal advisor to understand how to comply with your obligations under applicable law.

To comply with our transparency obligations, we explain how our cookies are used in our **Cookie Policy** and our **Cookies Settings Dashboard** sets out our list of cookies. We remind our Business Users to review the cookies placed on their website and to update their cookie banners accordingly.

Are there any jurisdictional nuances to Stripe's use of service providers in verifying the identity of Stripe's business users?

Germany

Stripe, through its service providers, may use information from infoscore Consumer Data GmbH to verify the identity of Stripe Business Users in Germany. Information about infoscore Consumer Data GmbH is available here.

Data Obtained from Third Parties

If you have been notified by Stripe that we obtained your data from a third party, the following applies:

Your Personal Data will be processed in accordance with Stripe's Privacy Policy, which describes:

the identity and the contact details of Stripe;

the contact details of Stripe's Data Protection Officer;

the purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing, which includes prospecting and direct marketing, as permitted under applicable law;

the recipients or categories of recipients of the Personal Data. In addition to the recipients mentioned in the Stripe Privacy Policy, Personal Data may be shared with Salesloft, Inc. as a processor of Stripe;

that Stripe intends to transfer Personal Data to a recipient in a third country and a reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available (see here and here for more information);

the period for which the Personal Data will be stored and/or the criteria used to determine that period;

the existence of the right to request from Stripe access to and rectification or erasure of Personal Data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability or any other applicable rights under data protection laws (see also here);

the right to lodge a complaint with a supervisory authority.

We may have obtained the following Personal Data from third parties: name, business contact details (e.g., email, phone number, social media handle), business address, company/employer information, role and position, and industry.

We use a number of third parties to obtain Personal Data from, including Cognism Limited, ZoomInfo Technologies Inc., API Hub, Inc. dba Clearbit, Crunchbase Inc., PitchBook Data, Inc., infoAnalytica, Inc., People Data Labs, Inc., and Dealroom.co. These third parties collect Personal Data as separate controllers in accordance with their own privacy policies. If you wish to have your data removed from their respective database(s), please contact those parties directly. Some of these parties may have obtained your data from publicly accessible sources.

We do not use Personal Data we have obtained from third parties for automated decision-making.

Where Stripe relies on legitimate interest to process your Personal Data, such legitimate interest may be:

B2B market research and analysis;

B2B prospecting and selling; and

B2B marketing and advertising.

Stripe Legal Bases Tables

What legal basis does Stripe rely on to process personal data as a data controller?

We rely upon a number of legal grounds to enable our use of your Personal Data. In short, we use Personal Data to facilitate the business relationships we have with our Business Users and End Users, to comply with our financial regulatory and other legal obligations, and to pursue our legitimate business interests. We also use Personal Data to complete transactions and to provide payment-related services to our Business Users.

Our table below provides a detailed overview of why and how we use your Personal Data.

For the purposes of the General Data Protection Regulation, we rely upon a number of legal bases to enable our processing of your Personal Data.

End Users

When you directly use an End User Service (such as when you sign up for Link, or make a payment to Stripe Climate in your personal capacity), for your personal use, we refer to you as an "End User."

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Provide our Services. To provide services to you, including delivery, support, personalization and messages related to the service.	Your name, contact information, payment information including Bank Account Information and Bank Payments, and/or payment card number, CVC code and expiration date.	Our **contractual necessity** to perform our contractual relationship with you, under applicable data protection laws.
For the provision of our services including Link, Atlas and Identity. When we process data based on your consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing based on such consent before the consent is withdrawn.	If you choose to use Link you agree to let Stripe store your payment method and related information so that you can more readily make purchases with Business Users who use Stripe to provide payment processing services (e.g. Stripe Checkout).	Based on **consent** in processing this personal information.
Card Products and Financial Products including Issuing and Treasury Direct	Your name, email address, phone number, postal	Our **legitimate interests** in promoting our products and in

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Services. We use your Personal Data to offer you card products and financial products and services under the Stripe brand and/or under the brand of a Business User.	address, transaction information, password, PIN or similar credentials, card PANs, age, DOB, credit card number, drivers license number, tax ID, cookie data, tags and beacons, IP address.	determining eligibility for and offer new Stripe products and services.
Provide cryptocurrency-related services, including enabling End Users with Link accounts to purchase cryptocurrency from licensed third-party cryptocurrency exchange providers using a variety of payment methods and save certain personal information to facilitate subsequent cryptocurrency-related transactions.	Your name, email address, date of birth, billing address, IP address, information related to your cryptocurrency wallet (including wallet identifier, access times, and IP address used to create and access the wallet), and information related to your cryptocurrency purchases, including your transaction history.	Based on consent in processing this personal information.
Offer our Services and Alert you of Changes to our Services. For example, through Stripe Capital we offer capital loans to certain users who can satisfy particular criteria and to help determine if you qualify for a loan or not. Such information will be processed prior to the offer of a loan in order to determine eligibility.	The name of the representative of business, physical address of business, and the borrower's Stripe ID. The rest of the data processed concerns business information and not personal data.	Our **legitimate interests** in promoting our products and in determining eligibility for and offer new Stripe products and services.
Fraud Detection Services. We use your Personal Data collected across our Services (e.g. Stripe Radar) to detect and prevent fraud against us, our Business Users and financial partners, including to detect unauthorized log-ins using your online activity.	**Transaction information**. This includes: name, email address, billing and/or shipping address, payment method information (such as credit or debit card number, bank account information or payment card image), merchant and location, purchase amount, date of purchase, and in some cases, some information about what you have purchased, phone number and tax-related ID.	Our **legitimate interests** in monitoring and detecting fraud to ensure we detect activity that can have a harmful effect on our End Users.

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
	This includes web browsing information, usage data, referring URLs, location, cookies data, device data and identifiers. **IP address and physical address.**	
Marketing and Advertising. We may use your Personal Data to assess your eligibility for and offer you other Services. We use End User Personal Data for interest-based advertising and marketing purposes. We do not share End Customer Personal Data to third parties for their marketing purposes unless you give us or the third party permission to do so.	Contact information including: name, email address, work phone number, and job title. Connection data such as IP address, and web behavior (page visited, length on page, etc.)	Based on **consent** in processing this personal information. Our **legitimate interest** in undertaking marketing activities to offer you products or services that may be of interest to you.
Compliance and Harm Prevention. We process and share Personal Data as we believe necessary: (i) to comply with applicable law, (ii) for compliance with rules imposed by payment method in connection with use of that payment method (e.g. network rules for Visa); (iii) to enforce our contractual rights; (iv) to secure or protect the Services, rights, privacy, safety and property of Stripe, you or others, including against other malicious or fraudulent activity and security incidents; and (v) to respond to valid legal process requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, which may include authorities outside your country of residence.	Any Personal Data we process, including information necessary for identity verification such as government-issued IDs or selfie images.	Where these processing activities or disclosures are necessary to comply with our legal obligations, for the protection of a person's vital interests, for reasons of public interest, for reasons of substantial public interest, or for the purposes of Stripe's or a third party's **legitimate interest** in keeping Stripe secure, preventing a breach of the law, harm or crime, enforcing or defending legal rights, claims, or obligations, facilitating the collection of taxes and prevention of tax fraud or preventing loss or damage.

End Customers

When you do business with, or otherwise transact with, a Business User (typically a merchant using **Stripe Checkout**, e.g. when you buy a pair of shoes from a merchant that uses Stripe for payment processing) but are not directly doing business with Stripe, we refer to you as an "End Customer."

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Provide our Services to Business Users, including to process online payment transactions or in-person checkout, to calculate applicable sales tax, to invoice and bill, and to calculate their revenue. If you are an End Customer, when you make payments to, send shopping cart reminders, get refunds from, begin a purchase or otherwise transact with a Business User through Stripe's Services or a Stripe-provided device, Stripe will receive your transaction information. Depending on how the Business User has integrated our Business Services, we may receive this information directly from you, the Business User or another service provider to you or the Business User.	**Transaction Information (including from Checkout, Payment Processing and Treasury/Issuing Use)**. Your name, email, billing and/or shipping address, payment method information (such as credit or debit card number, bank account information or payment card image), merchant and location, purchase amount, date of purchase, and in some cases, some information about what you have purchased, phone number and tax-related ID. The payment method information that we collect will depend upon the payment method that you choose to use from the list of available payment methods offered by the Business User as part of the "checkout" process for your purchase. We may also receive your transaction history with the Business User. **Transaction-Related Information / Purchase Interests.** Information typed into a checkout field that is not ultimately submitted to the Business User.	Our **legitimate interests** in providing the Stripe products and services. Stripe processes this personal data given its legitimate interest in improving the Services and where it is necessary for the adequate performance of the contract with the Business Users.
Provide our Services to Business Users, to order payment methods on a per-customer basis on behalf of the Business User, to implement fraud thresholds chosen by the Business User, and to verify your payment method.	**Verification Information**. Your age (when purchasing age restricted goods) or information about you being the person who is authorized to use a payment method. The information collected will be the information that you choose to share for these purposes, which may include your government ID, your photo, your live image, and Personal Data apparent from the physical payment method (e.g. credit card image).	Our **legal obligations** in respect of our financial and regulatory obligations.
Reduce fraud and enhance security. We will use Personal Data about your identity, including information that you provide, to perform verification Services for Stripe or for the Business Users that you are doing business with and to reduce fraud and enhance security.	In some cases you may provide a "selfie" along with an image of your identity document, and we will use technology to compare and calculate whether they match and can be "verified." We will use information from our service providers and our Services to help verify your identity and fraud prevention.	Based on **consent** in processing this personal information. Our **legitimate interests** in detecting, monitoring and preventing fraud and unauthorized payment transactions.

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Radar and Card Verification Services. We use Personal Data of End Customers to detect and prevent fraud for Business Users, including to detect fraudulent payment cards using payment card images and unauthorized log-ins using online activity. In providing such services, we may provide Business Users that have requested such services with limited Personal Data about End Customers so that the Business Users can assess the fraud risk associated with an attempted transaction by its End Customer. We may also use payment card images to improve our Business Services.	**Transaction information**. This includes: name, email address, billing and/or shipping address, payment method information (such as credit or debit card number, bank account information or payment card image), merchant and location, purchase amount, date of purchase, and in some cases, some information about what you have purchased, phone number and tax-related ID. This includes web browsing information, usage data, referring URLs, location, cookies data, device data and identifiers. **IP address and physical address**.	Our **legitimate interests** in detecting, monitoring and preventing fraud and unauthorized payment transactions.
Compliance and Harm Prevention. We share Personal Data as we believe necessary: (i) to comply with applicable law, (ii) to comply with rules imposed by payment method in connection with use of that payment method; (iii) to enforce our contractual rights; (iv) to secure or protect the Services, rights, privacy, safety and property of Stripe, you or others, including against other malicious or fraudulent activity and security incidents; and (v) to respond to valid legal process requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities, which may include authorities outside your country of residence.	Any Personal Data we process.	Our **legal obligations** where disclosures are necessary to comply with our legal obligations. Our **legitimate interest** in keeping Stripe secure, preventing a breach of the law, harm or crime, enforcing or defending legal rights, claims, or obligations, facilitating the collection of taxes and prevention of fraud or preventing loss or damage.

Representatives

When you are acting on behalf of an existing or potential Business User (e.g. you are a founder of a company, or administering an account for a merchant who is a Business User), we refer to you as a "Representative."

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Reduce fraud and enhance security. We will use Personal Data about your identity, including information that you provide, to perform verification Services for Stripe.	Onboarding and verification information that you choose to share for these purposes, which may include your government ID, photo, live image, and Personal Data apparent from the physical payment method (e.g. credit card image).	Our **legal obligations** in respect of our financial and regulatory obligations. We process Personal Data to verify the identity of the Representatives of our Business Users in order to comply with fraud monitoring, prevention and detection obligations, laws associated with the identification and reporting of illegal and illicit activity, such as AML (Anti-Money Laundering) and KYC (Know-Your-Customer) obligations, and financial reporting obligations.
Advertising. We may use and share Representative Personal Data with others so that we may advertise and market our products and services to you, including through interest-based advertising subject to any consent requirements under applicable law.	Contact information including: name, email address, work phone number, and job title. Connection data such as IP address, and web behavior (page visited, length on page, etc.)	Based on **consent** in processing this personal information.
Communications. We may send you email marketing communications about Stripe products and services, invite you to participate in our events or surveys, or otherwise communicate with you for marketing purposes, provided that we do so in accordance with applicable law, including any consent or opt-out requirements.	Contact information such as your name, email address, phone number.	Based on **consent** in processing this personal information. Our **legitimate interests** in responding to inquiries, sending Service notices, ensuring compliance with applicable laws, preventing fraud, improving our services and providing customer support.
Tax and Atlas (Incorporation) Services. We may use your Personal Data to file taxes on behalf of your associated Business User. If your Business User uses Atlas, we may use your Personal Data to submit forms to the IRS on your behalf and to file documents with other governmental authorities.	Your contact details, such as name, postal address, telephone number, and email address; and financial and personal information about you, such as your ownership interest in the Business User, your date of birth and government identifiers associated with you and your organization (such as your social security number, tax number, or Employer Identification Number). You may also choose to provide bank account information.	Our compliance **with legal obligations** in respect of our financial and regulatory obligations. We process Personal Data to verify the identity of the Representatives of our Business Users in order to comply with fraud monitoring, prevention and detection obligations, laws associated with the identification and reporting of illegal and illicit activity, such as AML (Anti-Money Laundering) and KYC (Know-Your-Customer) obligations, and financial reporting obligations. Our **contractual necessity** to perform our contractual relationship with you,

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
		under applicable data protection laws.

Visitors

When you visit a Site without being logged into a Stripe account or otherwise communicate with Stripe, we refer to you as a "Visitor." (e.g. you send Stripe a message asking for more information because you are considering being a user of our products).

PROCESSING PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASES
Communications. We use any contact information that you provide to us to respond to any inquiries or requests for information you made; and if you have asked about us or our Services, to send you marketing emails by either asking for your consent or providing you an opt out in any messages we send.	Contact information such as your name, email address, phone number. Information you have provided to us, such as the products you are interested in.	Based on **consent** in processing this personal information. Our **legitimate interests** in responding to inquiries, sending Service notices and providing customer support.
Advertising. When you visit our Sites, we (and our service providers) may use Personal Data collected from you and your device to target advertisements for Stripe Services to you on our Sites and other sites you visit ("interest-based advertising").	Information collected from cookies such as your device, browser ID, and pages on our website which you have visited.	Based on **consent** in processing this personal information. Our **legitimate interest** in undertaking marketing activities to offer you products or services that may be of interest to you.
Fraud Detection. We use your Personal Data collected across our Services to detect and prevent fraud against Stripe, our Business Users and financial partners.	**Advanced Fraud Signals information collected via cookies.** This includes web browsing information, usage data, referring URLs, location, cookies data, device data and identifiers.	Our **legitimate interests** in detecting, monitoring and preventing fraud and unauthorized payment transactions.

Data Processing Agreement

What is a Data Processing Agreement (DPA) and how can I get one with Stripe?

A Data Processing Agreement ("DPA") is a contract between a data controller and a data processor that describes the roles and responsibilities of the parties when personal data is processed. If you are a Business User, please visit our FAQs page here to learn more about our DPA. Please contact us or your account manager if you have any questions.

Information about Stripe Products

How do you implement Privacy by Design at Stripe?

Privacy by design aims at building privacy and data protection up front and into the design specifications and architecture of information and communication systems and technologies to facilitate compliance with privacy and data protection principles. We rely on our internal privacy team and a review process for any new product launch. We are dedicated at every level of product development —from engineering to product management—to making privacy a key consideration. This helps ensure that people can trust the Stripe products that they enjoy every day.

Stripe Identity

End Customers

If you have been asked to verify your identity or have verified your identity using Stripe Identity, please visit the support web pages here and here to learn more about our privacy practices for Stripe Identity. Alternatively, you can jump to the specific topics linked here:

- Stripe's role in controlling and processing identity data in the US
- Understanding Stripe Identity
- Biometric verification
- Consent to use my identity information
- Security of my identity data
- What data is collected
- Identity data retention
- How I delete my identity data

Business User That Requested Verification

If you are a Business User that is using or intends to use Stripe Identity, please visit the support web page here for additional guidance on what you can tell your users and here and here for additional guidance on privacy considerations for your business.

Stripe's Card Image Verification

If you have been asked by your merchant (i.e., a Stripe Business User) to scan your credit card before completing your requested transaction, please visit the support webpage here to learn more about Stripe's Card Image Verification.

Stripe Connect At a Glance

Description

Stripe Connect is a payment software your third party platform provider (Platform) may use to enable you to receive Stripe services (including payment processing) and/or receive payouts.

Data Controller/ Data Processor

Stripe acts as both a data controller and data processor for the Platform. The Stripe entity that acts as data controller/ data processor for data processed in Europe is Stripe Payments Europe Limited ("SPEL").

Personal Data

The personal data transmitted to Stripe usually involves first name, last name, address, identification number, e-mail address, IP address, telephone number, and other data necessary for payment processing.

Purpose

The transmission of the data is aimed at payment processing, ledger management, and fraud prevention. The Business User / Platform will transfer personal data to Stripe. The personal data exchanged between Stripe and the Business User / Platform may be transmitted to verification agencies, and Business User data may be shared with Platforms. This transmission is intended for the Platform to manage its ledger and for Stripe to conduct identity and risk checks.

Transfer

Stripe will pass on personal data to affiliates and service providers or sub-processors, if deemed necessary to carry out contractual obligations or for the data to be processed.

Privacy Policy

For full details please see the applicable Privacy Policy of Stripe.

I am a user with a Custom connected account. Does Stripe also collect information about my Custom connected account from a third party?

If you are a user with a Custom connected account, Stripe may collect additional information about your account to enable fraud detection and fulfill financial compliance requirements. These requirements for additional information come from our regulators or financial partners and are intended to prevent abuse of the financial system. Examples of missing data fields include your address, phone number, social security number, date of birth, employer identification number, or website URL. Stripe may leverage data we already have from one of your Stripe accounts or Stripe may fill in some of this information by receiving data from a third party. You may view the information that we are associating with your account and update or correct that information by contacting the platform or business that created your Stripe payment account. Please see Stripe's Privacy Policy for additional information.

What responsibilities do Connect platforms with custom accounts have to allow their users to update or correct information associated with their accounts?

You, the Platform, are responsible for all interactions with your Custom accounts and for collecting all of the information needed to verify the Custom account-holders. Since Custom account holders cannot log into Stripe, it is up to you to build the user dashboard and communication channels. You are responsible for actioning any request by a user to update or correct their Stripe Custom account information.

I am a user with a Custom connected account. Will data collected from a third party be visible to my customers?

Card networks and issuers use statement descriptors to identify payments on a cardholder's bank statement. Statement descriptors usually include information about the payment, such as the name and phone number of the seller. However, the exact information displayed is ultimately up to a cardholder's bank. If Stripe updates your account's business address, phone number, or email address, these fields may be displayed on the statement descriptor within the cardholder's bank statement. However, the exact information displayed is ultimately up to the card network or the cardholder's bank. If any information is incorrect, please reach out to the platform through which you receive charges to ensure you have provided them with the most accurate information about you and your business.

What are Stripe ACS, Transaction Authentication, and Behavioral Biometrics?

What is Stripe ACS?

Stripe ACS is Stripe's transaction authentication solution for card issuers (e.g., banks). Stripe ACS helps card issuers to authenticate transactions of cardholders when they are making payments online using their cards.

What is behavioral biometrics?

Behavioral biometrics is an innovative technology that can be used for the purpose of preventing fraud and identifying legitimate transactions. Behavioral biometrics leverages a combination of personal data and device characteristics to distinguish between legitimate customers and fraudsters or bots.

How is behavioral biometrics data collected and used in Stripe ACS?

This processing is designed to verify a cardholder's identity based on their behavioral biometric data which is modeled based on data collected during each authentication attempt.

This type of transaction authentication will typically observe interactions within a system or device to verify a cardholder's identity for the purposes of authenticating online payments. The following elements may be processed during the authentication process:

- Length of text field inputs
- Location of mouse pointer
- Modifier key details (e.g., CTRL, SHIFT)
- Timing and location of mouse clicks
- Timing and location of touch events
- Timing between keystrokes
- Window scroll position

For the purpose of fraud risk mitigation, this processing involves use of a device identifier cookie (Ndcd, Device ID, DID) that aims to accurately analyze biometrics data observed on a specific device. This cookie facilitates device detection in order to enhance fraud detection and prevention as well as to identify suspicious devices or devices that are behaving abnormally. This is a first party, strictly **necessary** cookie that is active on the touch.tech and touchtechpayments.com domains, and has a duration of 12 months. For more information on how we use cookies, please see **Stripe's Cookie Policy**.

Purpose of processing and Stripe's role

Stripe may process biometric data relating to cardholders in order to assist card issuers to authenticate payment transactions. This is done as part of Stripe's payment transaction authentication services provided to card issuers (including for the purposes of meeting **Strong Customer Authentication** requirements).

In providing these services to card issuers, Stripe acts as a data controller in relation to cardholder data. Please see Stripe's **Privacy Policy** to learn more about our use of personal data.

As part of providing this authentication services to card issuers, Stripe engages with a third party provider, Mastercard, which also acts as a data controller. See **Mastercard's Privacy Notice** for details on Mastercard's processing activities in this context.

Customers rights and choices

Upon initiating a transaction, cardholders will have the option of providing their consent to processing their behavioral biometrics data as part of the transaction authentication flow. This will be presented to the cardholder during the

checkout flow on the merchant's website or app when authentication is requested from the card issuer. Cardholders will have the option to withdraw their consent during each subsequent transaction flow.

To withdraw consent outside of a transaction flow, you can email **privacy-acs@stripe.com** with the subject matter line "Stripe ACS - *withdraw consent*". In your email to withdraw consent, please provide: (a) the first 6 digits of your card number as this enables Stripe to identify your issuing bank (please do not provide any digits other than the first 6 digits); and (b) the phone number (including the country code) registered with your bank account that is used for one-time passcodes.

We will action this withdrawal request as soon as possible after it is verified, but please note that this can take up to 10 working days as we may need to verify the request with your card issuer. You may also contact the card issuer in order for the issuer to implement this withdrawal of consent by engaging with Stripe.

To submit a request to exercise any of the other **rights** described in our Privacy Policy, you may contact Stripe at **privacy-acs@stripe.com**.

Promotional Emails Feature

For End Customers and prospective End Customers of our Business Users

What is the Promotional Emails feature?

Promotional Emails is a feature that gives Business Users who use "Stripe Checkout" services a new tool to enable sending email promotional content to their customers and prospective customers. When you visit a Business User's checkout page (that is powered by Stripe Checkout services), the Promotional Email feature will enable Stripe to collect information about your preferences to receive promotional emails from that merchant.

Promotional email preferences are collected whether or not you complete the purchase or are just a prospective End Customer. "Prospective End Customer" means you visited a Business User's site and expressed an intent to make a purchase by starting a purchase on the Business User's checkout page, but did not complete that purchase during that session. To be a "prospective End Customer" for the promotional email feature, you also need to have started to input your contact information into the checkout form, and then not delete that information prior to the end of the session.

If you, prospective End Customer, indicate permission to receive news and personalized offers by virtue of the opt-in/opt-out checkbox on your Business User's checkout form, the following personal data is provided to your Business User so that your Business User can contact you to remind you of the items you left in the checkout or to provide you news and personalized offers:

Email (if provided by you).

Items in your cart with that merchant (if any).

"Personalized offers" means promotional or marketing materials tailored to you, such as coupons or advertisements based on the items in your cart or (in some cases) your prior purchases from that Business User. Even if you opt-out of personalized offers by a Business User, if you do business with that Business User, they may still need to contact you in order to enable a purchase (e.g., for delivery or billing purposes) or in connection with customer support. Please see your Business User's privacy policy for more information.

What is Stripe's role (Data Processor/Controller) in the processing of my Personal Data?

For the Promotional Emails feature, Stripe acts as a **data processor** or service provider, meaning that Stripe is acting at the direction of the Business User that has implemented this Stripe provided feature. The Stripe entity that acts as a data processor for personal data is:

Stripe Inc. in the United States.

Stripe Payments Europe Limited outside of the United States, including Europe

What Personal Data Is Stripe Collecting?

Stripe's **Privacy Policy** describes in more detail the personal data that Stripe collects in connection with payment transactions.

What Personal Data is Shared by Stripe with the Business Users I use?

Whenever you complete a transaction on a Business User's website that uses Stripe services, as a service provider to that Business User, Stripe will share your contact information with that Business User. Business Users use the information that Stripe provides in accordance with its own privacy policy, including in connection with your purchase.

With the Promotional Emails feature:

If you complete a purchase with a Business User, in addition to the transaction-related information identified in our **Privacy Policy** (e.g., your contact and billing information and the details of your transaction), Stripe will also share with your Business User your personalized offers and news preferences as determined by the opt-in/opt-out checkbox from your checkout form.

If you are a prospective **End Customer** (you start a purchase with your Business User on their checkout form but do not complete that purchase), the personal data that we share with your Business User depends on the following:

If you have not inputted any personal data into your Business User's checkout form, then we will not share any personal data with that Business User.

If you have inputted personal data into your Business User's checkout form:

If the checkbox for receiving news and personalized offers is not enabled when you leave your Business User's checkout session, we will not share any of that personal data.

If the checkbox for receiving news and personalized offers is enabled when you leave your Business User's checkout session, we will share the following information with that Business User:

Email (if provided by you).

Items in your cart with that merchant (if any).

End Customers and prospective End customers should always review the privacy policy or notice of the Business Users they visit and do business with for information about the Business User's data collection practices and purposes outside of this Stripe feature.

Does Stripe share my personal data with other Business Users?

No. Stripe does not share personal data collected in connection with purchases (or attempted purchases) from one Business User's checkout with another Business User. Please see our Privacy Policy to learn more about our practices.

How do I stop promotional emails from a merchant?

Any offers or promotional emails that you receive as a result of a Business User's use of the Promotional Emails feature are sent by Business Users (or others identified in the message), and not by Stripe. I If you do not find value in receiving these emails, please contact the Business User you are receiving the messages from. Stripe requires that Business Users that choose to implement the Promotional Email feature also provide the option to unsubscribe or opt-out of receiving further promotional messages. It would be a breach of Stripe's terms of service for a Business User to not promptly comply with opt-out requests.

How Does the Data Collection and Transfer Work?

The Promotional Email feature does not use cookies or track you across Business Users. Information collected from the Business User's checkout page is transferred only to the Business User via API calls or webhooks. Webhooks are a way for Stripe to send the information to the Business User automatically upon their request. Your information provided at checkout is encrypted in transit using HTTPS and TLS. See **Security at Stripe** for more information.

How do I stop the sale of my personal data in connection with this feature?

Stripe does not sell your personal data. See our Privacy Policy for more information. The Promotional Emails feature is not the sale of personal data. Rather, Stripe acts as a processor (or service provider) to Business Users for the Promotional Email feature. Please contact your Business User to learn about their personal data practices and how you can exercise rights to stop the sale or processing of personal data provided under applicable law and/or their privacy policy.

Stripe requires that Business Users that choose to implement the Promotional Email feature also provide the option to unsubscribe or opt-out of receiving further promotional messages. It would be a breach of Stripe's terms of service for a Business User to not promptly comply with opt-out requests.

For Business Users

How to Use this Service as a Business User

If you are a business that is using or intends to use Stripe's Promotional Emails feature, please visit the **support webpage** for tips and guidance on information to share with your End Customers and prospective End Customers regarding privacy considerations in connection with the Promotional Emails feature for your business.

Stripe Delegated Authentication

Cardholders

You may be given the option to enable on-device biometric verification and provide your consent for Stripe to store your payment method details for future transactions that use the same card. Please visit our **support site** to learn more about our privacy practices for Stripe Delegated Authentication. Alternatively, you can jump to a specific topic here:

How is personal data used in Stripe Delegated Authentication?

How can cardholders provide and withdraw their consent for the storage of their payment method details?

Link

We offer you the opportunity to store your payment methods with us so that you can conveniently use it across certain merchants who are our Business Users – we call this "Link" (formerly known as "Remember Me"). When you choose to use Link, you agree to let us store your payment method so that you can more readily make purchases through Link with Business Users of our payment processing Business Services (e.g., name, card number, cvc, and expiration date). We will also collect other Transaction Data, including billing address, shipping address, email and phone number. Your payment method data is secured using PCI-DSS standards.

Should you not have used Link and receive an SMS in error due to an inaccurate number being inserted at the authentication flow stage you can opt out here and your personal data will be deleted.

Stripe Capital

Stripe Capital provides Business Users with access to fast, flexible funding so businesses can manage cash flows and invest in growth. Depending on your business's corporate structure, eligible Business Users may apply for one of two Stripe Capital products: a loan or a merchant cash advance ("MCA"). Loans are provided by Celtic Bank in partnership with Stripe Capital.

What information does Stripe process for Stripe Capital?

We use existing data linked to your Stripe Account to evaluate your business's eligibility for Stripe Capital. You may also be asked to link additional data sources, such as business bank accounts or business credit information, for Stripe to evaluate in order to receive funding through Stripe Capital. The following information may be considered prior to the offer of a loan or a MCA in order to determine eligibility, including:

- Payment processing volume
- Payment processing growth
- Chargeback rate
- Customer base
- Duration of relationship with Stripe
- Bank account balances
- Transaction history
- Business credit history

Where Stripe is satisfied that a Business User meets particular criteria established by Stripe and bank partners (as applicable), we will send the Business User an email and dashboard notification notifying them of their business's eligibility for potential funding and invite them to apply for a loan or a MCA.

Once you have received an offer and submitted an application to receive your financing, we will use this above listed information to verify your business's eligibility and where your application is approved, to disburse the loan or the MCA to your linked bank account.

The legal basis for using your information

We will use your data where its use is in accordance with our legitimate business interests. Analysis of our Business User's information helps us to manage our business for our legitimate interests. It allows us to:

- Verify the identity of our Business Users in order to comply with fraud monitoring, prevention and detection obligations, applicable laws associated with the identification and reporting of illegal and illicit activity, such as AML (Anti-Money Laundering) and KYC (Know-Your-Customer) obligations, and financial reporting obligations.
- Assess the level of financial risk to us, financial partners and to Business Users involved in offering Business Users a loan or MCA.
- Enhance our learning models to allow us to better tailor our loans or MCAs to, and decrease the risk to, you and other Business Users.

We will also process your data where it is necessary for a loan or MCA agreement that you have entered into or because you have submitted an application to receive funding so that you can enter into a loan or MCA agreement with us.

We may send you email marketing communications about Stripe Capital offers, provided we do so in accordance with applicable law, including any consent requirements.

Who does Stripe share information with?

Stripe does not share any Personal Data collected for Stripe Capital related to Business Users in the UK. In the future, Stripe may share your agreement data with third parties who purchase the right to receive repayments on your loan or MCA.

What is Stripe's role?

Stripe, Inc., or a wholly-owned subsidiary of Stripe, is the controller of your data.

For Business Users located in the UK, the joint controllers of your data are Stripe Payments Europe, Limited. ("SPEL") and Stripe Capital Europe Limited, Ltd. ("SCEL"). The loan or MCA provided under the loan agreement is solely provided by SCEL.

How do I opt-out of receiving Capital offers?

Business Users have the option to unsubscribe or opt-out of receiving Capital offers via the link included in Stripe Capital emails. Business Users may also opt-out of dashboard notifications via the settings page of the Stripe Dashboard. If you have any questions, please contact us.

Linked Financial Accounts

If you are an End Customer who has been asked to link your financial account using Stripe, please visit the support webpage here to learn more about our privacy practices. Or you can jump to the specific topics linked here:

- Linking my financial account and consent
- Data collected, stored, and shared from my linked account
- How Stripe accesses data from my linked account
- Relationship between Stripe and its service providers
- Data security
- Who can access data from my linked account and for what purposes
- Who will obtain my login credentials
- Requesting disconnection or data deletion
- Correcting my financial account information

Are there instances when Stripe receives non-Stripe transaction history?

Yes. For example, Stripe enables the Business User to import non-Stripe data through the Stripe Dashboard to consolidate their revenue data in one place. Learn more. Separately, Stripe may also obtain your account transactions from your financial account with your consent. Learn more.

Refunds to End Customer Bank Account

End Customers

If you have been asked to provide your bank account and other information to process a refund on behalf of your merchant (i.e., our Business User), please visit the webpage here to learn more about our privacy practices for end customer bank account refunds.

Business User that uses Stripe to Process Refunds

If you are a Business User that is using or intends to use Stripe to process refunds, please visit the webpage here for additional guidance on privacy considerations for your business.

Stripe Frontier

What is Stripe Frontier?

Frontier is an advance market commitment (AMC) that aims to accelerate the development of carbon removal technologies by guaranteeing future demand for them. It facilitates purchases from high-potential carbon removal companies on behalf of buyers. Learn more at https://frontierclimate.com/.

What information does Stripe Frontier collect?

We will collect any information you choose to provide to us, for example, through support tickets, emails or social media. When you respond to Stripe emails or surveys, we collect your email address, name and any other information you choose to include in the body of your email or responses. If you contact us by phone, we will collect the phone number you use to call Stripe, as well as other information you may provide during the call. We will also collect your engagement data such as your registration for, attendance of, or viewing of Stripe events and other interaction with Stripe personnel. See our privacy policy for more information.

What is the legal basis for processing Stripe Frontier information?

We rely on consent to process your data. Where you proactively reach out to Stripe and provide your data, Stripe will process your data based on Stripe's legitimate business interests (e.g. help answer your queries, and provide customer support). With your permission or where allowed by law, we use your personal data to market our services to you, invite you to participate in our events or surveys, or otherwise communicate with you for our marketing purposes, provided that we do so in accordance with applicable law, including any consent or opt-out requirements.

Is my data relating to Stripe Frontier transferred?

We are a global business. Personal Data may be stored and processed in any country where we do business. We may transfer your Personal Data to countries other than your own country, including to the United States. These countries may have data protection rules that are different from 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). See our privacy policy for more information.

What are my rights and choices with respect to the information collected for Stripe Frontier?

You may have choices regarding our collection, use and disclosure of your Personal Data. If you no longer want to receive marketing-related emails from us, you may opt-out via the unsubscribe link included in such emails or as described here. We will try to comply with your request(s) as soon as reasonably practicable. Depending on your location and subject to applicable law, you may have the following rights described here with regard to the Personal Data we control about you.

How do I exercise my rights as to Stripe Frontier?

EEA and UK . To exercise your rights, you may contact our DPO. If you are a resident of the EEA or we have identified Stripe Payments Europe Limited as your data controller, and believe we process your information within the scope of the General Data Protection Regulation (GDPR), you may direct your questions or complaints to the Irish Data Protection Commission. If you are a resident of the UK, you may direct your questions or concerns to the UK Information Commissioner's Office.

California . If you are a consumer located in California, please review the California Consumer Privacy Act ("CCPA") section of our Privacy Policy.

See our privacy policy for additional jurisdiction-specific provisions.

Any questions about Stripe Frontier and the processing of your data?

If you have any questions or complaints, please contact us.

Data Protection Officer

Does Stripe have a Data Protection Officer (DPO)?

Yes, Stripe has appointed a Data Protection Officer ("DPO"), who can and they can be reached via email.

Quebec Act Respecting the Protection of Personal Information

Who is Stripe's person in charge of personal information under the Quebec Act Respecting the Protection of Personal Information in the Private Sector, and how do I contact them?

Stripe's Chief Privacy Officer is the person in charge of personal information. You may contact them via email.

International Data Transfers

The detail below is provided for informational purposes. It is not intended to provide legal advice. Stripe urges Business Users to consult with counsel to familiarize themselves with the requirements that govern their specific situations.

How is Stripe dealing with international data transfers?

As a global business, Personal Data may be transferred to, and processed, in any country where we do business, where our service providers do business or if you use an international payment method or financial partner service, the countries in which that payment method or financial partner operates.

We may transfer your Personal Data to countries other than your own country, including to the United States. Stripe relies on a number of data transfer mechanisms to legalize the transfer of Personal Data around the globe.

Stripe continues to have appropriate safeguards and compliance measures to ensure an adequate level of protection of personal data transferred outside the UK, EEA and Switzerland. Stripe's measures may include:

- Transferring Personal Data from the originating to a country or recipient that has been deemed to have an adequate level of data protection by relevant privacy authorities, including the European Commission.
- The Standard Contractual Clauses ("SCCs") approved by the European Commision. SCCs are a transfer mechanism (in the form of a legal contract) used by Stripe to provide a legal mechanism to transfer EU personal data outside of the EEA/UK. These are required under EU data protection law (known as the GDPR) and are incorporated into our agreements.
- The UK International Data Transfer Addendum ("UK Addendum") issued by the UK's Information Commissioner's Office to provide a legal mechanism to transfer Personal Data from the UK. This mechanism is required under UK data protection law (known as UK GDPR) and is incorporated into our agreements,
- Other alternative data transfer mechanisms approved by relevant privacy authorities to enable the transfer of Personal Data to a third country (e.g., a new version or successor to the Privacy Shield).

We have recently published our online **Data Processing Agreement** ("DPA") to include the updated SCCs and the UK Addendum. The SCCs and UK Addendum are incorporated automatically into our online DPA. For more information, please see our **FAQs**.

Stripe respects the privacy of everyone that engages with our products and services, and we are committed to being transparent about our privacy processes and policies.To learn more about our commitment to privacy and data security, please see our **Privacy Policy**, the rest of the **Stripe Privacy Center**, and the **Stripe Security Center**.

We also want to highlight some of our supplementary measures to protect our Business Users' data from unauthorized access.

Stripe employs security controls and maintains and enforces a security program that addresses the management of security. We also perform risk assessments and implement and maintain controls for risk identification, analysis, monitoring, reporting, and corrective action. Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle. In addition, Stripe employees, agents, and contractors acknowledge their data security and privacy responsibilities under Stripe's policies.

Stripe applies technical and organizational measures that include the following:

- Physical access control to prevent unauthorized persons from gaining access to the data processing systems available at premises and facilities (including databases, application servers, and related hardware), where Personal Data are processed.
- Virtual access control to prevent data processing systems from being used by unauthorized persons.
- Data access control to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization.
- Disclosure control to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed.

Entry control to audit whether data have been entered, changed or removed (deleted), and by whom, from data processing systems.

Availability control to ensure that Personal Data are protected against accidental destruction or loss (physical/logical).

Separation control to ensure that Personal Data collected for different purposes can be processed separately.

By default, Stripe encrypts data at rest and data in transit. We further protect your data with tools like audit logs, access management policies and certifications as described on our **Payments** page in the section "Security and compliance at the core". Security controls implemented at Stripe include TLS 1.2 configuration of endpoints for data in transit, TLS and/or SSL encryption for HTTPS and regular testing of infrastructure components. Two-step authentication is available for an extra layer of security at Dashboard login.

We get requests for access to data from law enforcement, and we review each request with the goal of responding with the minimum amount of required information in response to legitimate, legally mandated requests.

If you have any questions, please **contact us**.

Does Stripe rely on the Privacy Shield?

We no longer rely on the Privacy Shield as a transfer mechanism for data transfers given the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield are no longer valid as a result of the *Schrems II* decision issued by the European Court of Justice on July 16, 2020. We do continue to commit to the principles of the Privacy Shield Framework and Stripe continues to certify that it adheres to the Privacy Shield Principles as it can still provide privacy protections to Business Users. To view Stripe's certification, please visit the Privacy Shield website.

We acknowledge the announcement of the EU-U.S. Data Privacy Framework in March 2022 and the release of the **Executive Order** on Enhancing Safeguards For United States Signals Intelligence Activities on 7 October 2022. We are committed to ensuring that our Business Users' data can continue to flow freely between the EU and the U.S. and we will continue to closely monitor the legal requirements and guidance from the US and the EU.

How do the SCCs and UK Addendum impact my organization?

SCCs are legal contracts entered into between parties that are transferring EEA Personal Data outside of the EEA. At present Stripe relies on the SCCs for transfers of EEA data in our services. We have updated our agreements to implement the modernized SCCs (where applicable).

How to get a copy of the SCCs or UK Addendum?

We can provide more information about the appropriate or suitable safeguards that we have in place, such as a copy of the SCCs on request.

If you are a business with a Stripe account located in the United States, the UK, the EEA or Switzerland, the SCCs and UK Addendum are incorporated into your DPA and form part of your Stripe Services Agreement.

If you have signed an older version of the SCCs (being those that were developed prior to the GDPR), these will remain valid for (i) transfers of Personal Data from the EEA and Switzerland until 27 December 2022, and (ii) transfers of Personal Data from the UK until 21 March 2024. Please contact us or your account manager and we will send you the latest DPA with the latest transfer mechanisms. Alternatively, on your acceptance of the DPA the SCCs incorporated into the DPA will replace any prior version of the SCCs you have signed.

How do the European Commission's new Standard Contractual Clauses impact my organization?

Standard Contractual Clauses ("SCCs") are legal contracts entered into between parties that are transferring EEA personal data outside of the EEA. At present Stripe relies on the existing SCCs for transfers of EEA data in our services. We have updated our agreements to implement the modernised SCCs (where applicable).

How to get a copy of the SCCs?

We can provide more information about the appropriate or suitable safeguards that we have in place, such as a copy of the SCCs on request.

If you are a Business User, we offer the modernised SCCs published in 2021 ("2021 SCCs") for cross-border transfers outside of the EEA and Switzerland. The older versions of the SCCs will continue to apply to transfers of personal data from the UK. We will continue to monitor regulatory requirements and guidance from the UK Information Commissioner's Office. If you have signed an older version of the SCCs, these will remain valid until 27 December, 2022. If you would like to sign the 2021 SCCs, you can reach out to us at any time.

Please contact us or your account manager for more information.

Your Rights and Choices

How do I exercise my data protection rights?

Depending on your location and subject to applicable law, you may have the followings rights:

- Right to access
- Right of rectification
- Right to data portability

- Right to restrict processing
- Right to object to processing
- Right to withdraw consent (where it is relied upon)
- Right to erasure/deletion
- Right to opt-out of receiving electronic communications from us
- Right to non-discrimination for exercising your rights
- Right to opt-out from a sale of personal information
- Right to opt-out of “sharing” under California privacy law (**learn more**)
- Right to limit the use or sharing of sensitive personal information (learn more)
- Right to appeal Stripe’s response to your data subject request

Please read this section to find out more about specific rights. To submit a request to exercise any of the rights described above, please reach out to us by **email**, or via our **form** or by physical addresses listed in **Contact Us**.

You have the right to complain to your local data protection authority if you are unhappy with our privacy practices.

How do I access my data?

If you are a Business User or Representative, you may login in to the Stripe Dashboard to view personal information shared with Stripe.

If you are the End Customer of a Business User that uses Stripe services, the Business User would be the correct party to respond to a data subject access request related to your transactional information.

Depending on your location and subject to applicable law, you may have the right to request confirmation of whether Stripe processes Personal Data relating to you, and if so, to request a copy of that Personal Data. If you are an End User or otherwise have a direct relationship with us, you may submit your access request by **email**, or through our **form**. Please note that we may need to verify your identity and your relationship with us before we can proceed with your request.

In addition, Stripe's **Data Access Tool** provides self-service access to some of the data from integrated Stripe products.

How do I unsubscribe from marketing emails?

If you are a Business User or Visitor, you may unsubscribe from Stripe marketing emails **here**. If you have any questions about how to opt-out of Stripe marketing communications, please contact us **here**.

If you are a Link user, you may opt-out from marketing-related emails by using the unsubscribe link in any marketing email you receive, or by managing your subscription preferences in the Link website. To manage your preferences log into your **Link account**, then navigate to your account settings. Turn “Marketing emails - Receive updates and deals from Link and its partners” on or off. Your email address will be opted out of email marketing communications as soon as possible.

When does Stripe continue to process data after it has received a deletion request or objection to the processing?

In certain circumstances, Stripe may be required by law to retain and process your Personal Data even after a deletion request or objection to the processing. For instance, Stripe is required to retain certain Personal Data it receives from its Business Users to satisfy legal obligations under Know Your Customer (KYC) and Anti-Money Laundering (AML) laws.

Stripe may also rely on compelling legitimate grounds to continue processing your Personal Data. Stripe may act on such grounds, for instance, when it takes steps to prevent fraud and financial crimes. When Personal Data is necessary to enable or maintain the integrity of Stripe's fraud detection and financial models, Stripe may not be able to honor requests to delete or stop processing that data. If Stripe honored such requests, fraudsters might take advantage of its willingness to do so to seek deletion of data related to their past fraudulent activities. Without such data, Stripe would be less able to recognize similar activities in the future.

What data may be shared or made available to enable me to see Stripe ads on other sites?

To enable visitors of Stripe.com to see Stripe ads on other sites, we use advertising cookies. The data that Stripe shares or makes available to enable this advertising includes identifiers, internet or other similar network activity, IP addresses, and device characteristics. Click the below links to learn more about the data that may be shared or made available to enable this feature. You can disable the toggle in the "advertising" section of our cookie settings page at any time.

Third Party Service	Data that we may share or make available	Service Description	Learn more
Facebook	Purchase Information, Web Activity, Sign-up information, IP address, device and browser characteristics, timestamps of visits	The Meta Pixel is a snippet of JavaScript code that allows Stripe to track visitor activity on your website. It works by loading a small library of functions which we use whenever a site visitor takes an action (called an event) that we want to	https://developers.facebook.com/docs/meta-pixel

		track (called a conversion).	
Reddit	Purchase Information, IP Address, Web clicks, Sign-up information.	The Reddit Pixel is a tool that helps Stripe better understand the customer journey so we can measure, optimize and re-engage audiences for Stripe ad campaigns. The Reddit Pixel is used to leverage website insights and optimize ad campaigns to reach qualified users and drive conversions.	https://redditinc.force.com/helpcenter/s/article/About-Reddit-Ads-conversion-tracking
Marketo	Web traffic, Web clicks,	Marketo allows for tracking of end-user page visits and clicks to Stripe landing pages and external web pages. These are recorded in Marketo as “Visit Web Page” and “Clicked Link on Web Page” activities.	https://experienceleague.adobe.com/docs/marketo-measure/using/home
Yahoo	Unique identifier, Web clicks,	Yahoo pixels are used to record many different types	https://developer.yahooinc.com/native/guide/native-dsp-migration-guide/pixels/

	timestamp of visits	of events for conversion tracking across Stripe sites. These can include clicks or page visits.	
Linkedin	URL's, referrer, IP address, device and browser characteristics, timestamps of visits.	The LinkedIn Insight Tag is a lightweight JavaScript tag. It is used on Stripe websites to enable features like website retargeting, conversion tracking, and website demographics.	https://www.linkedin.com/help/lms/answer/a423304/enable-first-party-cookies-on-a-linkedin-insight-tag?lang=en
YouTube	Web Activity, Sign-up information, IP address, device and browser characteristics, timestamps of visits	YouTube cookies track end-user page visits on Stripe sites in order to serve a more personalized ad experience on YouTube.	N/A

Does Stripe honor the Global Privacy Control (GPC) opt-out preference signal?

Yes. Global Privacy Control (GPC) is a signal that is sent by a web browser on your behalf that communicates your choice to opt-out of sharing for targeted advertisements. If you have enabled GPC on your browser, you will automatically be opted out of any "sharing" when you interact with our site. You can learn more about how to use opt-out preference signals by visiting the Global Privacy Control website.

Can I turn off tracking and advanced fraud signals?

Your web browser may allow you to manage your cookie preferences, including deleting or disabling Stripe cookies. If you choose to disable cookies, keep in mind that some features of our Site or Services may not operate as intended. Disabling cookies will not disable the collection of advanced fraud signals, which we use to prevent fraud on Stripe. The collection of this data is controlled by the Business User that integrated with Stripe. If a Business User seeks to disable this data collection, they can find instructions to do so through Stripe's documentation. You can take a look at the help section of your web browser or follow the links below to understand your options for disabling cookies.

- Google Chrome
- Microsoft Internet Explorer
- Microsoft Edge
- Safari
- Firefox
- Opera

You can learn more about how businesses can disable collection of advanced fraud signals in our documentation for disabling advanced fraud detection.

How do I delete my account?

You can close your Stripe account from the Settings page on the Dashboard. You can read more about that on our support page: Close a Stripe account.

Please be aware that we will delete some, but not all, of the information that we hold, for the reasons explained below.

As a provider of payment services, Stripe is required to comply with many regulations, including anti-terrorism and anti-money laundering laws. These regulations and laws may require Stripe to retain transactional records associated with Business Users for a prescribed period of time after the close of the business relationship. You can read more about our underwriting obligations in our Privacy Policy.

How do I delete my Custom Connect account?

If you have a Custom Connect account, your account is managed by a Platform / Business User. They are the party responsible for managing payments for you and responding to your query; therefore we recommend reaching out to them for assistance.

How do I delete my Express Connect account?

If you have an Express Connect account, your account is managed by a Platform / Business User. They are the party responsible for managing payments for you and responding to your query; therefore we recommend reaching out to them for assistance.

How long will Stripe keep my data?

Stripe keeps Personal Data as necessary to achieve the purposes listed here. To determine the appropriate retention periods for different categories of Personal Data, we consider various criteria such as the jurisdiction you are located in, the nature of our relationship with you, the types of products or services being offered or provided to you, the nature and sensitivity of your Personal Data, retention requirements under applicable laws and regulations, and other legitimate interests we may pursue through retaining your Personal Data, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, and promoting our products and services as appropriate and as permitted by applicable law and agreements.

For most jurisdictions, Stripe will generally keep Personal Data we obtain from our Business Users for a period of five or more years from the end of the business relationship with you, or the date of the last transaction, whichever is later.

The table below outlines different categories of personal data collected, along with the retention period or the criteria used to determine that period.

CATEGORIES OF PERSONAL DATA COLLECTED	RETENTION PERIOD OR THE CRITERIA USED TO DETERMINE THAT PERIOD
Non-sensitive Identifiers (e.g., name, postal address, IP address, email address, account name)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, and promoting our products and services as appropriate and as permitted by applicable law and agreements.
Categories of personal information described in Cal. Civ. Code § 1798.80(e) (such as name, address, telephone number, credit card or debit card number)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, and promoting our products and services as appropriate and as permitted by applicable law and agreements.
Characteristics of protected classifications under California or federal law (e.g., gender and age noted in ID documents that you submit so that	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and

Stripe can verify your identity on behalf of your merchant - a.k.a. our business user)	financial crimes, enforcing and defending our legal rights, and complying with valid legal process requests from courts or competent authorities.
Commercial information (e.g., transaction data that the merchant you choose to do business with - a.k.a. our business user - may receive)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, and promoting our products and services as appropriate and as permitted by applicable law and agreements.
Biometric information (e.g., biometric identifiers from photo IDs and selfies used to confirm your identity)	No longer than 1 year, or upon revocation of your consent, whichever is earlier.
Internet or other electronic network activity information (e.g., certain information about devices and browsers across certain business user sites that use Stripe, and usage data)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, and promoting our products and services as appropriate and permitted by applicable law and agreements.
Geolocation Data (e.g., IP addresses)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, and complying with valid legal process requests from courts or competent authorities.
Audiovisual (e.g., visual, audio, or similar information, like photos you submit so that Stripe can verify your identity on behalf of your merchant – a.k.a. our business user)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities, improving the quality of our services, promoting our products and services as appropriate and as permitted by applicable law and agreements.
Professional or Employment-Related Information	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) make certain employment and performance-related decisions; (3) address future hiring needs; (4) ensure health and safety in the workplace; (5) conduct certain administrative tasks, including to administer benefits; and (6) pursue our legitimate interests, including enforcing and defending our legal rights and complying with valid legal process requests from courts or competent authorities.

Education information that is not publicly available as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)	For the duration necessary for Stripe to: (1) comply with legal obligations under applicable law; (2) make certain employment and performance-related decisions; (3) address future hiring needs; (4) conduct certain administrative tasks, including to administer benefits, and; (6) pursue our legitimate interests, including enforcing and defending our legal rights and complying with valid legal process requests from courts or competent authorities. For biometric data, Stripe will not retain it for longer than 1 year or upon your revocation of consent, whichever is earlier.
Sensitive personal information, as defined by California law. Learn more	For information regarding your government IDs (including the sensitive data therein) and your location data, Stripe will retain that data for the duration necessary to: (1) comply with legal obligations under applicable law; (2) provide the Stripe services, and; (3) pursue our legitimate interests, including detecting and preventing fraud and financial crimes, enforcing and defending our legal rights, complying with valid legal process requests from courts or competent authorities. Where we rely on consent to collect your other sensitive personal information (e.g., financial account login credentials), Stripe will no longer retain this data upon your revocation of consent.

California Privacy Rights Metrics

The following includes aggregate metrics of data subject rights requests received between January 1, 2022 and December 31, 2022. This data reflects requests received from individuals in California and may also include requests from individuals who do not reside in California.

- Number of “request to know” received, complied with in whole or in part, or denied: 5
- Number of “requests to delete” received, complied with in whole or in part, or * denied: 7,118
- Average number of days taken to respond to a request to know or delete: 1 day

There are instances where Stripe may deny a “request to know,” such as when the data subject fails to reply with information that would allow Stripe to accurately authenticate their identity to locate their data.

Even if we receive a “request to delete,” Stripe may nonetheless retain personal data where permitted by law, including to comply with our legal obligations. For example, as a provider of payment services, Stripe is required to comply with many regulations, including anti-terrorism and anti-money laundering laws. These laws require Stripe to retain certain information associated with Stripe users for a prescribed period of time after account closure. Learn more about our retention obligations in our Privacy Policy.

Due to the nature of Stripe’s products and services, when we receive a “request to delete,” our process is to direct the requestor to a page to action their request depending upon the relationship they have with Stripe. We also offer data subjects the opportunity to contact us, should they have any questions or concerns.

Request to Opt Out of Sale

Stripe does not “sell” personal information as defined by the California Consumer Privacy Act (CCPA). Learn more.

What is the Privacy Policy for Stripe Media Services?

The Privacy Policy for Stripe Media Services (Media Privacy Policy) describes how Stripe collects and processes personal data in order to provide the Stripe Media Services, including Stripe Press, Increment, and Works in Progress. We encourage you to read our Media Privacy Policy to learn more.

Does Stripe localize storage of data in India?

Personal Data may be processed either locally in India or in any other country where we have operations or where we engage service providers, to the extent permitted under applicable laws of India. The entire payment system data will be stored only in India in accordance with the RBI data localization guidelines.

Where can I lodge my complaint on data handling in India?

If you have any questions or complaints regarding the treatment of your Personal Data in India, please contact our Nodal Officer and Grievance Officer:

Name - Yogender Singh

Email Address - complaints-in@stripe.com

Address - 2nd Floor, WeWork Pavilion, Church Street, Bengaluru 560001, Karnataka, India

For more information about complaint handling, please visit here.

Separately, for law enforcement requests, please contact LERequests@stripe.com.

Notification IT Rules 2021

We are required to inform you that in case of non-compliance with rules and regulations, our Privacy Policy or user agreement, we have the right to terminate your access or usage rights immediately or remove non-compliant information or both, as the case may be.

Cookies & Other Technology

How does Stripe use cookies?

We use cookies to (1) ensure that our services function properly, (2) prevent and detect fraud and violations of our terms of service, (3) understand how visitors use and engage with our website and (4) analyze and improve our services. Depending on your relationship with Stripe and the domain you are visiting, different cookies apply. For instance some cookies are set on a public Stripe or Link domain, some on the Stripe Dashboard or a Link settings page, and some on the payment page available to end users who make payments using Stripe services, including Link.

Cookies play an important role in helping Stripe provide personal, effective and safe services. Please be mindful that we change the cookies periodically as we improve or add to our services. For more information, please see our Cookie Policy.

What is Stripe.js?

Stripe.js is a JavaScript library that businesses use to integrate Stripe and accept online payments (corresponding iOS and Android SDKs enable the same use cases). Stripe uses Stripe.js to facilitate fraud prevention technologies and the use of its Link payment services on the websites of Business Users.

For fraud detection, Stripe.js uses cookies, including `__stripe_mid`, `__stripe_sid`, and `m`, to collect signals differentiating legitimate behavior from fraudulent behavior. For example, fraudsters and bots often spend less time on Business Users' pages than legitimate End Customers. We are able to detect this behavior and use it in evaluating the risk that a transaction is fraudulent.

When you visit a site that uses Stripe, you might see this fraud prevention activity in a privacy report or tracker list on your web browser. Stripe doesn't—and won't—share or sell the fraud data it collects using Stripe.js to advertisers. Stripe works to keep this fraud detection data secure and ensure it does not leave Stripe infrastructure. It is exchanged between the following Stripe-controlled hosts:js.stripe.com, m.stripe.network, and m.stripe.com, and access to this data is tightly restricted to a small number of Stripe employees whose security permissions are regularly reviewed. You can read more about how Stripe uses data for fraud prevention in our Privacy Policy.

Stripe also uses the Stripe.js library to implement cookies and similar technology such as `pay_sid`, `link.auth_session_client_secret`, and `elements_session` to enable Link to remember users' information for faster checkout across Stripe merchant sites and to collect analytics related to Link's implementation on checkout pages.

You should regularly review the Stripe cookies that are placed on your website and other data collected by Stripe.js. You should consult your counsel regarding how best to disclose this data collection to your customers, including by updating your cookie banner. But, here is a paragraph you could add to your privacy disclosures if they do not already include such information:

We use Stripe for payments, analytics, and other business services. Stripe collects identifying information about the devices that connect to its services, including via cookies and similar technologies. Stripe uses this information to

operate and improve the services it provides to us, including for fraud detection, authentication, and analytics related to the performance of its services. You can learn more about Stripe and read its privacy policy at ***https://stripe.com/privacy.***

What are advanced fraud signals?

Stripe's advanced fraud detection looks at signals about device characteristics and user activity indicators that help distinguish between legitimate and fraudulent transactions. These signals are highly indicative of fraud and power Stripe's fraud prevention systems, such as Radar. The signals are securely transmitted to Stripe's backend by periodically making requests to the m.stripe.com endpoint.

You can learn more in our documentation for **advanced fraud detection**.

Why are advanced fraud signals not ad tracking?

Stripe only uses these advanced fraud detection signals to enable secure payments and prevent fraud. We don't use this data to build individual profiles or share or sell it to third-party advertisers.

You can read more about how we use this data in our **Privacy Policy**.

How does Stripe remember payment method details for Link?

Link (formerly known as "Remember Me") lets end users save and reuse their payment information for faster checkout at thousands of online businesses that use Stripe. When an end user makes a purchase via a Business User (i.e., merchant) that enables Link, the end user can ask Stripe to remember their payment method details, such as credit and debit card details. If an individual chooses to be remembered, Stripe will remember the end user's email address, phone number, shipping address, and payment method details for future Link transactions.

The payment method details for future transactions may be remembered across multiple Stripe Business Users. Generally, once the cookie is set, the end user may make "1-click" purchases using Link when you check out, which means that Stripe will automatically populate the end user's saved information into their checkout on their behalf, and use the information to complete the transaction faster.

If the end user enters their phone number or email address during a future Link transaction, Stripe will authenticate the end user by sending the end user a One Time Passcode (OTP), e.g. via an SMS message or email. If the end user correctly enters the OTP, Stripe or the Business User will set a cookie in the end user's browser, indicating that the end user has been authenticated. If the end user does not enter the OTP, or elects to "log out" of their Link session then the cookie won't remember the end user.

A cookie is only stored in a specific browser on a specific device. If an end user wishes to make 1-click purchases in a different browser or on a different device, they must go through the OTP authentication process for the new browser or device combination.

After 90 days, it will be necessary for the end user to re-complete the OTP process. The end user may also proactively remove the cookie by clearing cookies in their browser or by selecting the “log out” option when this option is presented in checkout.

If an end user no longer wishes for Stripe to remember their payment method details when they check out in the future, the end user may use the **self-service deletion tool**. Alternatively, the end user may also contact Stripe support to make this request.

The description above describes how an end user may control how their information is stored and used to check out. However, this does not affect the other contexts in which Stripe may store and use end user information. In particular, Stripe may store and use such information as described elsewhere on this Privacy Center - including for purposes such as for advanced fraud detection.

What obligations should Link users keep in mind relating to cookie technology on their sites?

Based on your integration choice (e.g., for Link in Elements), you may have legal responsibilities associated with cookies and similar technology that Stripe uses for fraud detection and/or authentication purposes.

You should always check with your legal counsel to understand how you should comply with applicable legal obligations with setting cookies and similar technology. This section has information to keep in mind.

Stripe cookies or similar technology are set on your domain (e.g. on your checkout flow) from the Stripe.js library. The current Stripe cookies from the Stripe.js library include fraud prevention cookies like `__stripe_mid`, `__stripe_sid`, and `m`, and also end-user authentication cookies like `pay_sid` and `__Host-LinkSession`.

You should regularly review the Stripe cookies that are placed on your website to ensure that your own privacy disclosures tell your end users about this type of data collection, and also update your cookie banner accordingly after reviewing the cookies placed on your website. Here is a paragraph you could add to your privacy disclosures if it does not already include such a disclosure:

*We use Stripe for payment, analytics, and other business services. Stripe collects identifying information about the devices that connect to its services, including via cookies. Stripe uses this information to operate and improve the services it provides to us, including for fraud detection and authentication. You can learn more about Stripe and read its privacy policy at **https://stripe.com/privacy**.*

Does Stripe use reCAPTCHA to protect its website from fraud and abuse?

Yes, some of the Stripe sites may implement Google **reCAPTCHA** Enterprise to help prevent fraud and abuse. Information collected by Google is used to provide and improve reCAPTCHA Enterprise and for general security purposes. Use of reCAPTCHA Enterprise is subject to Google’s **Privacy Policy** and **Terms of Use**.

Contact Us

Contact our Privacy team

If you have any outstanding privacy questions after reviewing the privacy policy, please don't hesitate to reach out to us by **email**, or through our **form**.

If you'd like to send us physical mail, please send to:

Stripe, Inc.

354 Oyster Point Boulevard

South San Francisco, California, 94080, USA

Attention: Stripe Legal

Stripe Payments Europe Limited

1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland

Attention: Stripe Legal

Where can I learn more about Stripe's security practices?

Visit our **security page** to learn more about Stripe's security practices. You should **contact us** immediately if you become aware of any unauthorized use or any other breach of security regarding the Stripe services.

Stripe Services Agreement
Stripe Connected Account Agreement
Stripe Payments Company Terms
Acquirer Terms
- Cross River Bank
- PNC Bank
- Wells Fargo Bank

Issuing Bank Terms
Payment Method Terms
User Bank Debit Authorizations
Restricted Businesses
Other Products and Programs
- Stripe Terminal Device EULA

- Stripe Terminal Purchase Terms
- Stripe Terminal Reseller Terms
- Stripe Atlas Agreement
- Stripe Climate Contribution Terms

Stripe Apps

- App Developer Agreement
- App Marketplace Agreement

Privacy

- Privacy Policy
- Cookies Policy
- Privacy Shield Policy
- Service Providers List
- Data Processing Agreement
- Stripe Privacy Center

Intellectual Property

- Intellectual Property Notice
- Marks Usage

E-SIGN Disclosure

Licenses

Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

Stripe's Restricted Business Intellectual Property ("IP") Notice Process

Last updated: October 29, 2020

By registering with Stripe, businesses confirm that they will not use Stripe Services (as defined **here**) in connection with certain businesses or business activities. We've outlined those on our **Restricted Businesses** page. One type of restricted activity is the sale of any good or service that infringes the trademark, copyright, or other intellectual property ("IP") rights of any third party. Stripe understands that the protection of IP is important to our mission to increase the GDP of the internet, and we take claims of IP infringement seriously.

To that end, if you are an IP owner (or an authorized representative of an IP owner), and you have a good-faith belief that a business is using Stripe Services in connection with the sale of goods or services that infringe your IP rights, please let us know by filling out this **notice** ("IP Notice") and sending it to us by email to ip-notice@stripe.com. While we will consider and review any complete IP Notice submitted to us through that process, unfortunately we can't do that for other communications that are submitted to us in other ways, or that are incomplete.

Before you submit your IP Notice to us, we'd ask that you consider several points:

Does the business at issue have its own IP notice process? If so, we'd ask that you use that first, and include with your IP Notice to us any documentation that you submitted to the business directly notifying them of the allegedly infringing goods or services.

Are you sure that the business in question is using Stripe? Often businesses will claim to use Stripe that are not in fact using our Services. Moreover, it is not uncommon that references to Stripe will remain visible in a website's source code long after a business is no longer using Stripe. For that reason, we ask that you please include in your IP Notice any evidence that suggests that the business is **currently** using Stripe Services. Successful test purchases are encouraged (but not required), as evidence of a test purchase can be extremely helpful in that regard. That said, please do **not** include card information as part of your IP Notice.

Is the business using Stripe Services in connection with the sale or distribution of specific infringing goods or services (such as infringing movies or software)? Or does your IP Notice allege that some aspect of the business overall (such as its name, its logo, its website design, etc.) is infringing? If the latter, we'd encourage you to resolve your dispute directly with the business: as a provider of economic infrastructure, Stripe is not in a position to mediate those types of IP disputes.

Is this the right forum? In other words: does your notice allege that a business is using Stripe Services in connection with the sale of goods or services that infringe IP rights? Or does it allege something else? By

way of example, please do not use this process to notify us about: 1) other (non-IP) alleged violations of our Restricted Business terms; 2) instances where you allege that Stripe itself is infringing your IP; or 3) instances where you allege that material that resides on a system or network controlled or operated by Stripe or one of our affiliated companies allegedly infringes your copyright (please contact our DMCA Agent for that: DMCA Agent; Stripe, Inc.; 354 Oyster Point Boulevard, South San Francisco, California, 94080; phone: 628-250-1970; email: dmca@stripe.com).

Once we receive a complete IP Notice, we will consider and review the allegations in it, and will let you know if we need any more information. Several points to keep in mind as we do that:

Please do not submit multiple notices on the same allegedly infringing goods or services, as doing so could slow down our review.

Please understand that in our role as a provider of economic infrastructure, we do not take our supportability decisions lightly, and will need to make sure that any supportability decision we make is rigorously reviewed and factually sound.

Please be aware that as part of our investigation we may share the IP Notice with the allegedly infringing business.

Following our review of your IP Notice, we will decide whether the business remains eligible to use the Stripe Services. But note: we cannot "take down" or remove any allegedly infringing offerings of goods or services of the business. All we can do is continue (or not) to provide our payment processing and related Services to the business --- which means that the "result" of our investigation into an IP Notice may not be visible in many respects to the outside world. While we will try to keep you informed of the status of our review of your IP Notice, the most that we will likely be able to convey is whether Stripe Services are (or are not) currently being used to support the ongoing sale of the specific goods or services that were the subject of your IP Notice.

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

- Cross River Bank
- PNC Bank
- Wells Fargo Bank

Issuing Bank Terms

Payment Method Terms

User Bank Debit Authorizations

Restricted Businesses

Other Products and Programs

- Stripe Terminal Device EULA
- Stripe Terminal Purchase Terms
- Stripe Terminal Reseller Terms
- Stripe Atlas Agreement
- Stripe Climate Contribution Terms

Stripe Apps

- App Developer Agreement
- App Marketplace Agreement

Terminal

Treasury

Build a Stripe App

stripe

Stripe's Mark Usage Terms

Last updated: June 12, 2023

We appreciate that many of our Users — as well as our partners, vendors, and others who may be connected to us in other ways — will often want to mention their connection with us, and will often want to use our name or logo to do so. These Mark Usage Terms (what we'll call the "Marks Usage Terms") are intended to clarify how our Users may do that. To answer any questions you may have about these Marks Usage Terms or if you want to use our marks other than to note that you are a Stripe User (perhaps in your checkout flow), please email us at trademarks@stripe.com.

Some uses of our Marks will require an express license. In those cases, the terms of that license will govern. Other uses of our Marks will be governed by separate agreements or terms. In those cases, the terms of those agreements will govern. These Marks Usage Terms are intended to cover everything else, and will govern any uses of our Marks that are not governed by any other license or agreement.

Before we get to the specific do's and don'ts, some general points:

> First, let's define what we're covering here. When we use the collective term "Marks" (or the singular "Mark"), that means any of our names, logos, icons, design elements, trade dress, or anything else (whether registered or unregistered) that we may use to identify and distinguish our goods or services from those of others. We have many marks, but here are a few examples:
>
> > Our Stripe word mark;
> >
> > Our Stripe stylized mark:
> >
> > stripe
> >
> > Our Stripe logo:
> >
> > 

As noted above, these are just examples, not an exhaustive list of our marks. That said, we chose them as examples in part because each one is registered in at least the U.S. Patent and Trademark Office (if not other trademark offices as well). If you would like to use one of our marks other than as noted above, please email us at trademarks@stripe.com.

> Our Marks are valuable assets. In following these Marks Usage Terms and using our Marks, you are acknowledging that we are the sole owner of the Marks and that you will not interfere with our rights in the Marks (including challenging our use, registration, or application to register a Mark). You also acknowledge that the goodwill derived from your use of any of our Marks inures to our benefit, and belongs to us.

The permission that we're giving you to use our Marks is limited, in several ways:

- You can only use our Marks as expressly permitted under these Marks Usage Terms.
- The permission we're giving you is non-exclusive (meaning, we can give it to others) and non-transferable (meaning, you can't).
- We may update these Marks Usage Terms from time to time, and you will update your use of the Marks to conform to any changes we make within a reasonable time after we give you notice of the change.
- We may review your use of our Marks on your website and require changes if necessary to comply with these Marks Usage Terms.
- We may terminate your permission to use our Marks at any time (and at our discretion). Upon termination you agree to promptly stop all use of the Marks (for example, by removing any Marks from any websites or applications).

So what then can you do and not do? As a general rule, you may use our Marks to truthfully convey information about your goods or services, but not in a way that will imply endorsement by us of your goods or services, or otherwise cause consumer confusion. To help you understand what that means in practice, we have created this non-exhaustive list of what you can and can't do:

Do:

- Use our Marks only on the portion of your website or application that directly relates to our services (such as on a checkout page using our payment processing services).
- Use our Marks consistent with any style guidelines (describing such things as size, color, or relative placement) that we may give you (and update your use to conform to any changes in those style guidelines within a reasonable time after we give you notice of the change).
- Use our Stripe word mark without alteration in text to truthfully and accurately refer to us or our goods or services.

Don't:

- Use our Marks except as described in these Marks Usage Terms (or otherwise agreed inwriting).
- Modify or alter our Marks in any way. For example, don't shorten or abbreviate any of the Marks (many of them are relatively short to begin with!), or use any of them in plural, possessive, foreign-language translation, or otherwise modified forms.
- Misrepresent your relationship with us, or use our Marks in any way that is misleading, or that would imply our endorsement or sponsorship of your goods or services (or anybody else's goods or services).
- Use our Marks more prominently than your own (or any others').
- Use our Marks in any way that is unrelated to us or our goods or services.
- Use our Marks on any tangible merchandise, including any promotional, marketing, swag, or other physical items.
- Add anything in such close proximity to our Marks as to create a new mark with its own distinct commercial impression.
- Use or incorporate any of our Marks in your own trademark, service mark, trade dress, trade name, website name, domain name, corporate name, or social-media handle (or any other source-identifying use), or use any trademark, service mark, trade dress, trade name, website name, domain name, corporate name, or social-media handle (or any other source-identifying use) that is likely to be confused with any of our Marks.

Use our Marks to show Stripe or our goods or services in any disparaging or derogatory light, or in any way that may be damaging to our brand or to our interests in the Marks.

Use a ™ or ® in conjunction with our Marks. Different countries have different rules on this and in order to be consistent across regions we don't require your use at this time.

stripe

United States

English (United States)

Products

Atlas
Billing
Capital
Checkout
Climate
Connect
Corporate Card
Data Pipeline
Elements
Financial Connections
Identity
Invoicing
Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Solutions

Enterprises
SaaS
Marketplaces
Creator Economy
Finance Automation
Platforms
Ecommerce
Crypto
Embedded Finance
Global Businesses

Integrations & Custom Solutions

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Resources

Support Center
Support Plans
Guides
Customer Stories
Blog
Annual Conference
Contact Sales
Privacy & Terms
Licenses
COVID-19
Sitemap
Cookie Settings
Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

E-SIGN Disclosure

1. Scope of Disclosure.

This disclosure ("**Disclosure**") applies to all notices, disclosures, statements, and other communications that Stripe, Inc. or its affiliates ("**Stripe**") provide to you regarding Stripe products and services ("**Services**"). It also applies to agreements governing your use of the Services, and communications under them. All these communications and agreements are collectively referred to as "**Communications.**"

By submitting an application or opening an account to use the Services, you agree to this Disclosure and confirm your consent to (a) receive Communications electronically; and (b) the use of electronic signatures. If you choose not to consent to this Disclosure or if you withdraw your consent, you may be unable to use the Services.

2. Communications that are covered.

Examples of Communications include:

- Any disclosure statement governing your use of the Services;
- Any disclosure required by Law;
- Billing statements, receipts and account history reports;
- Letters, notices and alerts regarding the Services and any changes to the Services;
- Federal and state tax statements and documents; and
- Other disclosures, notices and communications in connection with (a) your application for the Services; (b) your Stripe Account; (b) account maintenance; or (d) servicing and collection of funds.

This Disclosure applies to all Communications that Stripe provides to you on its behalf or on behalf of its service providers, Financial Partners and their affiliates.

3. Methods of Providing Communications.

Unless Law otherwise requires, or Stripe otherwise agrees, Stripe may provide Communications to you by (a) posting them on the Stripe Website; (b) notifying you through the Services, your Stripe Dashboard or any Stripe application; (c) sending a text message to the mobile phone number listed in the applicable Stripe Account; (d) sending an email to the email address listed in the applicable Stripe Account; or (e) delivering them in another electronic format. Charges may apply to Communications sent by text or other electronic means.

4. Electronic Signatures.

Stripe may execute Communications electronically. If Stripe requests, you will execute Communications electronically. You also agree that Communications you or Stripe sign electronically will have the same legal effect as a signed physical document.

5. Hardware and Software Requirements.

In order to access, view, sign and retain electronic Communications that Stripe provides to you, you must have:

- An up-to-date device (e.g., computer, tablet, or mobile phone) which has internet access;
- A current, compatible web browser, including the current or immediately preceding version of Chrome, Internet Explorer, Firefox, Safari and Edge;
- A valid email account;
- An operating system on your device capable of receiving, accessing and displaying Communications in electronic form via text-formatted email or gaining access to the Stripe Website using a supported browser, including any necessary software (e.g., Adobe to read PDF documents); and
- If you wish to store or print any Communications, a device capable of storing and printing Communications.

If you use a spam filter that blocks or re-routes emails from senders not listed in your email address book, you must add relevant Stripe email accounts to your email address book.

6. Accessibility.

If you are having problems viewing or accessing any Communications, please **contact us**.

7. How to Withdraw Your Consent.

Where offered, you may disable electronic Communications in your Stripe Dashboard, by responding to the Communication with “STOP”, or by following instructions in the Communication. Stripe will confirm when you have successfully unsubscribed. You may also request assistance by texting “HELP” and following the instructions in the Communication.

In addition, you may withdraw your consent to receive electronic Communications, or to electronic signatures, under this Disclosure by writing to Stripe at “ATTN: Stripe Support, 354 Oyster Point Blvd, South San Francisco, CA 94080” or by contacting Stripe at **stripe.com/contact**. Your withdrawal of consent to receive electronic Communications will be effective after Stripe has had a reasonable period of time to process your withdrawal.

By disabling or withdrawing your consent to electronic Communications, you will no longer receive them from Stripe, but you may be disabling important security controls on your Stripe Account, you may increase the risk of loss to your business, and your ability to use the Services may be adversely affected or terminated.

8. Requesting Paper Copies.

You can request paper copies of electronic Communications from Stripe by contacting Stripe at **stripe.com/contact**. In your request, please specify the Communication you would like to receive in paper form, and your current mailing address.

9. Updating Contact Information.

It is your responsibility to keep your contact information, including your primary email address, current. You can update your primary email address and other contact information by logging into your **Stripe Dashboard**.

10. U.S. Federal Law.

If you are located in the U.S., you acknowledge and agree that the Services are subject to the federal Electronic Signatures in Global and National Commerce Act ("**E-SIGN Act**"), and that you intend that the E-SIGN Act will apply to validate your ability to engage electronically in transactions related to the Services.

Stripe Services Agreement

Stripe Connected Account Agreement

Stripe Payments Company Terms

Acquirer Terms

- Cross River Bank
- PNC Bank
- Wells Fargo Bank

Issuing Bank Terms

Payment Method Terms

User Bank Debit Authorizations

Restricted Businesses

Other Products and Programs

- Stripe Terminal Device EULA
- Stripe Terminal Purchase Terms
- Stripe Terminal Reseller Terms
- Stripe Atlas Agreement
- Stripe Climate Contribution Terms

Stripe Apps

- App Developer Agreement
- App Marketplace Agreement

Privacy

- Privacy Policy
- Cookies Policy
- Privacy Shield Policy

stripe

United States

English (United States)

Products

Atlas
Billing
Capital
Checkout
Climate
Connect
Corporate Card
Data Pipeline
Elements
Financial Connections
Identity
Invoicing
Issuing
Link
Payments
Payment Links
Payouts
Pricing
Radar
Revenue Recognition
Sigma
Tax
Terminal
Treasury

Solutions

Enterprises
SaaS
Marketplaces
Creator Economy
Finance Automation
Platforms
Ecommerce
Crypto
Embedded Finance
Global Businesses

Integrations & Custom Solutions

App Marketplace
Partner Ecosystem
Professional Services

Developers

Documentation
API Reference
API Status
API Changelog
Build a Stripe App

Resources

Support Center
Support Plans
Guides
Customer Stories
Blog
Annual Conference
Contact Sales
Privacy & Terms
Licenses
COVID-19
Sitemap
Cookie Settings
Your Privacy Choices

Company

Jobs
Newsroom
Stripe Press
Become a Partner

stripe

Stripe Payments Company Licenses

STATE	AUTHORITY
AK	Department of Commerce, Community & Economic Development, Division of Banking & Securities
AL	Securities Commission
AR	Securities Department
AZ	Department of Financial Institutions
CA	Department of Financial Protection and Innovation
CO	Division of Banking
CT	Department of Banking
DC	Department of Insurance, Securities, and Banking
DE	Office of the State Bank Commissioner
FL	Office of Financial Regulation
GA	Department of Banking and Finance
GU	Department of Revenue and Taxation
HI	Division of Financial Institutions
IA	Division of Banking
ID	Department of Finance, Securities Bureau
IL	Department of Financial & Professional Regulation, Division of Financial Institutions
IN	Department of Financial Institutions
KS	Office of the State Bank Commissioner
KY	Department of Financial Institutions

STATE	AUTHORITY
LA	Office of Financial Institutions
MA	Division of Banks
MD	Commissioner of Financial Regulation
ME	Bureau of Consumer Credit Protection
MI	Department of Insurance and Financial Services
MN	Department of Commerce
MO	Division of Finance
MS	Department of Banking and Consumer Finance
NC	Office of the Commissioner of Banks
ND	Department of Financial Institutions
NE	Department of Banking & Finance
NH	Banking Department
NJ	Department of Banking and Insurance
NM	Financial Institutions Division
NV	Department of Business and Industry, Financial Institutions Division
NY	Department of Financial Services
OH	Department of Commerce, Division of Financial Institutions
OK	Banking Department
OR	Division of Financial Regulation
PR	Bureau of Financial Institutions
PA	Department of Banking and Securities
RI	Department of Business Regulation, Division of Banking
SC	Office of the Attorney General
SD	Division of Banking
TN	Department of Financial Institutions

TX	Department of Banking
UT	Department of Financial Institutions
VA	Bureau of Financial Institutions
VI	Division of Banking, Insurance and Financial Regulation
VT	Department of Financial Regulation, Banking Division
WA	Department of Financial Institutions
WI	Department of Financial Institutions
WV	Division of Financial Institutions
WY	Department of Audit, Division of Banking

Alaska

Alaska Department of Commerce, Community, and Economic Development

For Alaska Residents Only:

If your issue is unresolved by Stripe Payments Company 888-926-2289, please submit formal complaints with the State of Alaska, Division of Banking & Securities.

Please download the form here:

https://www.commerce.alaska.gov/web/portals/3/pub/DBSGeneralComplaintFormupdated.pdf

Submit formal complaint form with supporting documents:

Division of Banking & Securities
PO Box 110807
Juneau, AK 99811-0807

If you are an Alaska resident with questions regarding formal complaints, please email us at dbs.licensing@alaska.gov or call Nine Zero Seven Four Six Five Two Five Two One

California

California Department of Financial Protection and Innovation

If you have complaints with respect to any aspect of the money transmission activities conducted at this location, you may contact the California Department of Financial Protection and Innovation at its toll-free telephone number, 1-866-275-2677, by email at consumer.services@dfpi.ca.gov, or by mail at the Department of Financial Protection and Innovation, Consumer Services, 2101 Arena Boulevard, Sacramento, CA 95834.

RIGHT TO REFUND

You, the customer, are entitled to a refund of the money to be transmitted as the result of this agreement if Stripe Payments Company does not forward the money received from you within 10 days of the date of its receipt, or does not give instructions committing an equivalent amount of money to the person designated by you within 10 days of the date of the receipt of the funds from you unless otherwise instructed by you.

If your instructions as to when the moneys shall be forwarded or transmitted are not complied with and the money has not yet been forwarded or transmitted, you have a right to a refund of your money.

If you want a refund, you must mail or deliver your written request to Stripe Payments Company at 354 Oyster Point Boulevard, South San Francisco, California, 94080. If you do not receive your refund, you may be entitled to your money back plus a penalty of up to $1,000 and attorney's fees pursuant to Section 2102 of the California Financial Code.

Customer Assistance

California customers using Stripe Payments Company's money transmission services may receive live customer assistance by calling 888-926-2289 (toll-free) Monday - Friday (excluding federal holidays) between the hours of 8:00 AM and 6:00 PM PST.

Colorado

Colorado Division of Banking

CUSTOMER NOTICE

Entities other than FDIC insured financial institutions that conduct money transmission activities in Colorado, including the sale of money orders, transfer of funds, and other instruments for the payment of money or credit, are required to be licensed by the Colorado Division of Banking pursuant to the Money Transmitters Act, Title 11, Article 110, Colorado Revised Statutes.

If you have a Question about or Problem with YOUR TRANSACTION – THE MONEY YOU SENT: You must contact the Money Transmitter who processed your transaction for assistance. The Division of Banking does not have access to this information.

If you are a Colorado Resident and have a Complaint about THE MONEY TRANSMITTER – THE COMPANY THAT SENT YOUR MONEY: All complaints must be submitted in writing. Please fill out the Complaint Form provided on the Colorado

Division of Banking's website and return it and any documentation supporting the complaint via mail or email to the Division of Banking at:

Colorado Division of Banking
1560 Broadway, Suite 975
Denver, CO 80202
Email: DORA_BankingWebsite@state.co.us
Website: https://banking.colorado.gov/industry/money-transmitters

District of Columbia

District of Columbia Department of Insurance, Securities, and Banking

For complaints directly to the District of Columbia Department of Insurance, Securities, and Banking please send correspondence to:

District of Columbia Department of Insurance, Securities, and Banking
1050 First Street NE, Suite 801
Washington, DC 20002
Telephone Number: (202) 727-8000
https://disb.dc.gov/

Florida

Florida Office of Financial Regulation

For complaints, directly to the Florida Office of Financial Regulation, please send correspondence to:

Florida Office of Financial Regulation
200 E. Gaines Street
Tallahassee, FL 32399-0381
Toll-Free Number: 1-800-848-3792

Illinois

Illinois Department of Financial and Professional Regulation

For complaints directly to the Illinois Division of Financial Institutions, please send correspondence to:

Illinois Department of Financial and Professional Regulation
Division of Financial Institutions
Consumer Complaints

555 W. Monroe, Suite 500
Chicago, IL 60661
Toll-Free Number: 1-888-473-4858

Maryland

Maryland Commissioner of Financial Regulation

The Commissioner of Financial Regulation for the State of Maryland will accept all questions or complaints from Maryland residents regarding Stripe Payments Company (NMLS #1280479) at 1100 N. Eutaw Street, Suite 611, Baltimore, MD 21201 or at 1-888-784-0136. See https://nmlsconsumeraccess.org/ for licensing information.

Minnesota

Minnesota Department of Commerce

Per Minnesota Statute 53B.27, Stripe Payments Company ("SPC") is hereby notifying you of your right to voluntarily disqualify yourself from sending or receiving money transfers. This disqualification ("Disqualification") is valid for one (1) calendar year from the time the request is received until three hundred sixty five (365) days have passed, unless you request to SPC that the Disqualification be in effect for a time period longer than one (1) calendar year. You must submit a written notice either by electronic mail to notices@stripe.com, or by certified mail to Stripe Payments Company, Attn: Legal Department, 354 Oyster Point Boulevard, South San Francisco, California, 94080, in order for you to request for your Disqualification to be terminated ("Termination Request"). Once the Termination Request is processed by SPC, it is considered effective immediately thereafter.

Per Minnesota Statute 53B.27, SPC is providing you with the following consumer fraud warning: please always remain alert to the possibility of fraud. You can always go to https://www.consumer.ftc.gov/scam-alerts to receive the latest information and practical tips from the United States Federal Trade Commission- a consumer protection agency. To report fraud or suspected fraud as it relates to your transactions with SPC, please dial the following toll free number: (888) 926-2289.

New York

New York Department of Financial Services

Stripe Payments Company is licensed and regulated as a money transmitter by the New York State Department of Financial Services.

New York customers can direct unresolved complaints to:

Consumer Assistance Unit
NYS Department of Financial Services

One Commerce Plaza
Albany, NY 12257
1-877-BANK-NYS (1-877-226-5697)
https://www.dfs.ny.gov/complaint

Right to Refund for New York Residents

You, the customer, are entitled to a refund of the money to be transmitted as the result of this agreement if Stripe Payments Company does not forward the money received from you within 10 days of the date of its receipt, or does not give instructions committing an equivalent amount of money to the person designated by you within 10 days of the date of the receipt of the funds from you unless otherwise instructed by you.

If your instructions as to when the moneys shall be forwarded or transmitted are not complied with and the money has not yet been forwarded or transmitted you have a right to a refund of your money.

If you want a refund, you must mail your written request to Stripe Payments Company at Legal Department, 354 Oyster Point Boulevard, South San Francisco, California, 94080.

Texas

Texas Department of Banking

After first contacting Stripe Payments Company either online (notices@stripe.com) or by phone at 1-888-926-2289, if you still have an unresolved complaint regarding the company's money transmission activity, please direct your complaint to:

Texas Department of Banking
Non-Depository Supervision Division
2601 North Lamar Boulevard
Austin, Texas 78705-4294
Toll free: (877) 276-5554 or email msb@dob.texas.gov
Fax #: (512) 475-1288
https://www.dob.texas.gov/money-services-businesses/how-file-complaint

Washington

Washington Department of Financial Institutions

Per Washington Administrative Code 208-690-205(2), Stripe Payments Company is providing you with the following consumer fraud warning: fraudulent transactions may result in the loss of your money with no recourse. To report fraud or suspected fraud as it relates to your transactions with Stripe Payments Company, please dial the following toll free number: (888) 926-2289.

Stripe Services Agreement

- **Stripe Connect**
  - Platform Agreement
  - Account Agreement
- **Products and Programs**
  - Stripe Atlas
  - Stripe Automatic Currency Conversion
  - Stripe Climate
  - Climate Contribution Terms
  - Stripe Corporate Card
  - Stripe Customer Portal
  - Stripe Data Pipeline
  - Stripe Financial Connections
  - Stripe Identity
  - Stripe Issuing
  - Stripe Tax
  - Stripe Partner Program
  - Stripe Radar
  - Stripe Rewards
  - Stripe Verifications
  - Stripe Shop
  - Stripe Terminal
  - Terminal Purchase Terms
  - Terminal Reseller Terms
  - Terminal Device EULA
  - Stripe Treasury - Connected Accounts
  - Stripe Treasury - Platforms
- **Financial Services Terms**
  - Stripe Payments Company
  - Wells Fargo
  - PNC Bank
- **Payment Method Terms**
- **Restricted Businesses**
- **Privacy**
  - Privacy Policy
  - Cookies Policy
  - Privacy Shield Policy
  - Service Providers List
  - Data Processing Agreement
  - Stripe Privacy Center
- **Intellectual Property**
  - Intellectual Property Notice
  - Marks Usage
- **Stripe Apps**

App Developer Agreement

App Marketplace Agreement

Licenses