

Payment Labs Privacy Policy

Last Updated: April 20, 2026

Payment Pro Logistics, LLC, doing business as Payment Labs (“Payment Labs,” the “Company,” “we,” “us,” or “our”), respects your privacy and commits to protecting it through our compliance with the practices described in this online privacy notice (“Privacy Notice,” “Privacy Policy,” “Policy,” or “Notice”). Please read this policy carefully. Capitalized terms not defined herein shall have the meanings prescribed to them in the Payment Labs Terms of Service.

About This Privacy Policy

This notice describes our practices for collecting, using, maintaining, protecting, and disclosing (“processing”) your personal information when you use our products and services (the “Services”), such as when you:

- Visit a website of ours that links to this privacy notice (“Website(s)”), including the following:
 - www.paymentlabs.io
 - www.paymentlabs.com
 - www.prizepayments.com
 - www.mallo.io
- Download or use our mobile application (our “App”) or any other application that links to this Notice
- Engage in a transaction with us, for example, by making a purchase
- Subscribe to or engage with our promotional emails, text messages or SMS services, and other electronic communications
- Interact with our social media pages
- Click on our ads posted on third-party sites
- Engage with our affiliates
- Communicate with our service representatives or features (including via chat functions, email, text, or phone)
- Visit us at our physical locations (where we may collect personal information related to your visit, including for example, video security footage or your use of our Wi-Fi network)
- Use our Services anywhere we collect information from you and refer to this Privacy Notice

This Notice also applies to personal information we collect from third parties about you. This Policy does not apply to websites, apps, videos (embedded or direct links), or other content (each a “Linked Site”) to which we link that are not operated by us. Linked Sites have their own personal information collection and use practices, and we are not responsible for those practices. We encourage you to read each Linked Site’s privacy disclosures to understand how your personal information is processed.

What is Personal Information?

“Personal information” (sometimes called “personal data”) is a broadly defined term whose legal definition varies across jurisdictions. When used in this Policy, “personal information” includes information that is reasonably capable of identifying a particular individual (including through their device) either alone or when combined with information from other sources.

How We Receive Your Information.

In certain cases, Payment Labs receives limited personal information — specifically, your email address and payment parameters — from a business client ("Company") that has engaged Payment Labs to process payments on its behalf. For that specific data, the Company acts as a data controller and is responsible for the lawfulness of its disclosure to Payment Labs. Payment Labs acts as a data processor with respect to that data and processes it only as directed by the Company. All additional personal information that Payment Labs collects directly from you — including identity verification data, tax documentation, bank account details, and biometric data — is collected and controlled by Payment Labs independently to fulfill its own legal, regulatory, and compliance obligations.

What Information Do We Collect?

The personal information we collect about you depends on the nature and context of your interaction with our Company and Services. It may also depend on various choices you make about how to use the Services we offer, the functionality and features you choose or enable, your location, the devices you use to interact with our services, and applicable law.

The following describes the personal information we collect about you and the way we collect it.

Personal Information You Give to Us

The personal information about you that we collect includes, but is not limited to, the following:

- **Contact Information.** For example, your first and last name, email address, phone number, physical address, job title, and other contact information you provide.
- **Account and Other Identifiers.** For example, your username, screen name, handle, account ID, assigned user ID, customer number, or similar identifier that can be used to identify you or your account.
- **Account Verification Information.** For example, your account security questions and answers.
- **Transaction History.** For example, the purchases and purchase tendencies associated with you or your account. This may also include information that you provide for the purposes of sending Payouts (see “Financial and Transaction Information” below). It also includes the records of payments made to you, the amounts paid to you, and other information associated with payment transactions.
- **Consumer Credit Information.** For example, your credit score, credit history, and creditworthiness.
- **Financial Information.** For example, your salary, income, assets, debts, or other financial information.

- **Coarse Location Information.** A general approximation of your location that is not based on global position system (GPS) information.
- **Social Media Content.** If you interact with our social media pages, we will receive information related to those interactions.
- **Employment Candidate Information.** Individuals applying for employment or other positions in our workforce may provide personal information in connection with the candidacy for employment. Personal information may include contact information, work history, education history, salary preferences, résumé information, and C.V.
- **Other Personal Information You Provide.** If you provide us personal information other than that described above, we will collect it and use it for the purposes for which you provide it or other related purposes.
- **Information on Identification and Tax Documents.** If you provide us with copies of your driver’s license, government issued ID, or tax documents, we will collect and use the information contained thereon for the purposes for which you provide it or other related purposes.

Sensitive Personal Information. Some jurisdictions have defined certain categories of personal information as “sensitive.” We may collect the following categories of sensitive personal information when you provide it to us or allow us to collect it based on your interaction(s) with us.

- **Payment processing information.** For example, the form of payment, payment card number and details, bank account number, payment service provider, and other payment information you provide.
- **Precise location information.** A specific determination of your location using longitudinal and latitudinal coordinates determined by GPS.
- **Social Security number.**
- **Driver’s license number.**
- **Government ID card number.**
- **Tax identification number.**
- **Account access credentials.** For example, your username and password.

Personal Information We Derive Through Your Use of Our Services

We automatically collect certain information about your (and your device’s) interaction with our Services using various data-gathering and tracking technologies. These technologies include cookies, web beacons, tags, scripts, software development kits (SDKs), and similar tools. The information we collect using these technologies includes, without limitation:

- **Browsing and Search History.** Information about the content you view and searches you make on our Website(s).
- **Website Log and Usage Data.** Data related to our pages you viewed, the services and features you used or interacted with, your browser type and details about any links or communications with which you interacted.
- **App Log and Usage Data.** Including app launches, taps, clicks, scrolling information, music listening data, video views, save points in videos, games, or songs, and other information about your interaction with our App(s).

- **Advertising Metrics.** Data about the advertisements you have viewed on our Website and/or Mobile App.
- **Diagnostic Data.** Such as crash logs, launch time, hang rate, energy use, and other information collected for measuring technical diagnostics.
- **Device information.** Data about the device used to access our Services. Device information includes device identification numbers, application identification numbers, advertising identifiers, device location information, mac address, hardware model, internet service provider, and mobile carrier.

Because browser-based “Do Not Track” signals have yet to gain widespread acceptance, our Websites currently do not respond to those signals.

Cookies and other Tracking Technologies

"Cookies" are small data files that are sent to your web browser when you access a website, and the files stored on your device's hard drive. We use "session" cookies to keep you logged in while you use the Payment Labs' Website(s), to track your preferences and to track trends and monitor usage and web traffic information on the Website(s). These are erased when you close your browser. We use "persistent" cookies to relate your use of our Service to other information about you and store information about your preferences to make your user experience consistent and customized. For example, we may create a persistent cookie that includes some basic information about you, like your favorite website locations and whether customer support responded to your inquiry. These cookies stay on your hard drive until you erase them, or they expire and associate your information with your account even if you are logged out.

Most browsers automatically accept cookies, but you can change your settings on the browser settings to refuse cookies or prompt you before accepting cookies. You can also use your browser settings or other tools to delete cookies you already have. However, if you disable or refuse cookies, then certain features of the Website(s) may be inaccessible or not function properly.

Our cookies do not, by themselves, contain personal information, and we do not combine the general information collected through cookies with other personal information to tell us who you are. As noted, however, we do use cookies to identify that your web browser has accessed aspects of the Service and may associate that information with your account if you have one.

Certain features of the Website(s) may use local shared objects (or "flash cookies"). Flash cookies are small files similar to browser cookies that collect and store information about your preferences and where you browse and what you look at on the Website(s). Flash cookies are not managed by the same browser or device settings that are used for browser cookies. You may adjust your Adobe Flash Player settings to prevent flash cookies from being placed on your hard drive.

This Privacy Policy covers our use of cookies only and does not cover the use of cookies by third-parties. We do not control when or how third-parties place cookies on your computer. For example, third-party websites to which a link points may set cookies on your computer.

We may use "clear GIFs" (aka "web beacons" or "pixel tags") or similar technologies, on our Service or in our communications with you to enable us to know whether you have visited a part of our Service or received a message. A clear GIF is typically a one-pixel, transparent image (although it can be a visible image as well), located on a website or in an email or other type of message, which is retrieved from a remote website on the Internet enabling the verification of an individual's viewing or receipt of a website or message.

We do not automatically collect personal information, but we may tie personal information with the automatically collected information using the above tools or information collected from other sources.

We may also log information using digital images called web beacons on our Service or in our emails. We may use web beacons to manage cookies, count visits, and to learn what marketing works and what does not. We may also use web beacons to tell if you open or act on our emails. We also use third-party analytics services to collect usage data from our Website(s) in order to help us understand how users are interacting with our Website(s). Third-party analytic services are used to determine approximate location information, and events that occur regarding our Services, such as how often you use our Services. This information, including your IP address, is transmitted and stored by 3rd parties as determined by us.

Financial and Transaction Information

We use a licensed third-party payment service provider as an Accounts Payable Automation Platform ("APAM") to process Payouts (the "MT Service"). Our MT Service collects information directly from you when you use it. This information may include, without limitation:

- **Payee Information.** Information concerning Payee Users to whom payments are made through the Services, including but not limited to, name, physical address, e-mail address, phone number, VAT ID, Social Security number or U.S. Taxpayer number (for U.S. Payees, as applicable), government issued identification number, any Payee information which may be required under applicable tax forms for transferring and receiving payments, country of residence, bank account numbers, IBAN, SWIFT code (or alternatively, account details at other third-party payment processing services such as provided by PayPal, as applicable), payment preferences, session IP address, and supplemental documentation as may be required by Payors of their Payees that may contain Personal Information (such as a copy of their government-issued identification card, personal bank statements or other documentation serving as proof of identity or valid address), and any other Personal Information provided to us by either Payors or Payees.
- **Payor Information.** Information concerning Payor Users (including authorized personnel of Payor), namely their company name and affiliation, physical address, e-mail

addresses and login credentials to our Services, bank account numbers (or alternatively, their account details at payment processing services such as PayPal, as applicable), payment preferences and transaction history (to the extent that any such information is personally identifiable to any particular persons).

Who Provides Us with Personal Information?

We mostly collect personal information directly from you or based on your interaction with our Websites or App. However, we also may collect personal information from third-party sources, including:

- **Advertising Networks**
- **Internet Service Providers**
- **Data Analytics Providers**
- **Operating Systems and Platforms**
- **Identify Verification Service Providers**
- **Information Databases**
- **Social Media Platforms**
- **Business Partners**
- **Government Entities**
- **Our Affiliates**
- **Security Providers**
- **Our APAM**

What Do We Do with Your Personal Information?

We may use your personal information for a variety of reasons. Depending on how you interact with our Services, these include:

- To deliver our Services to you.
- To validate your identity as necessary to perform our contract with you, maintain security, and comply with applicable law.
- To send you important information, such as information about your account and membership options, including expiration and renewal notices.
- To send you marketing and promotional communications, as permitted by law.
- To facilitate communications between you and Us or between you and another User.
- To respond to your requests related to our Services.
- To maintain and improve the security and performance of our Services.
- To anonymize, aggregate, or de-identify your personal data (so it can no longer identify you) in furtherance of conducting research and analysis.
- To develop and improve our current and future offerings and your experience.
- To make strategic decisions concerning our business operations.
- To deliver targeted advertising and to measure its effectiveness.
- To display third-party ads, including sharing information with entities who display third-party ads.
- To determine the effectiveness of promotional campaigns.

- To enforce, and review compliance with, the legal terms that govern our offerings in furtherance of our legitimate interest in ensuring adherence thereto.
- To comply with our legal obligations under applicable laws.
- To protect the rights, safety, and property of the Company, our users, and third parties.
- In any other way we may describe when you provide the information. • For any other purpose with your consent.

When we process personal data about you to comply with legal requirements or to perform our obligations under a contract with you or with our customer through whom you use our offerings, failure to provide such data may prevent or delay our fulfillment of these obligations.

When and With Whom Do We Share Your Personal Information?

We may share your personal information with the following:

- **Business Operations Providers.** Including cloud computing service providers, internet service providers, data backup and security providers, functionality and infrastructure providers, and similar service providers.
- **Payment and Billing Providers.** Including our APAM.
- **Website and Mobile App Operations Providers.** Including hosting providers, performance monitoring providers, user account registration and authentication providers, testing providers, analytics providers, chat feature and user commenting providers, content optimization providers, social media sharing plugin providers, and similar providers.
- **Marketing and Advertising Providers.** Including advertising, direct marketing, and lead generation providers, affiliate marketing program providers, retargeting platforms, data brokers, ad networks, marketing consultants, and similar services providers.
- **Legally Required Parties.** Persons to whom we are required by law to provide information, such as pursuant to a subpoena or a court order.
- **Professional Service Providers.** Including lawyers, accountants, consultants, security professionals, and other similar parties when disclosure is reasonably necessary to comply with our legal and contractual obligations, prevent or respond to fraud or abuse, defend ourselves against attacks, or protect the rights, property, and safety of us, our customers, and the public.
- **Reorganization.** Persons involved in the consideration, negotiation, completion of a business transaction, including the sale, merger, consolidation, acquisition, change in control, transfer of substantial assets, bankruptcy, or reorganization, and any subsequent integration.
- **Authorized Disclosures:** To any party when you request or authorize us to share it.

We may also gather aggregated data about individuals and disclose the results of such aggregated (but not personally identifiable) information to our partners, service providers, advertisers, and/or other third parties for marketing or promotional purposes.

How Long Do We Keep Your Personal Information?

We will retain your personal information only for so long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information; the potential risk of harm from unauthorized use or disclosure of your personal information; the purposes for which we process your personal information and whether we can achieve those purposes through other means; and the applicable legal requirements. In some circumstances, you may ask us to delete your data. Additionally, we may anonymize your personal information (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

How Do We Protect Your Personal Information?

We have implemented and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect your personal information from unauthorized access, destruction, use, modification, or disclosure. However, no security measure is perfect, so we cannot guarantee the security of your personal information.

Examples of our security measures include the following:

- Restricting access to personal information to those workforce members who need to know it.
- Training our workforce members about the importance of privacy and security of personal information.
- Implementing internal policies and procedures governing the collection, use, retention, and disclosure of personal information.

We strongly encourage you to set strong passwords for your User account(s), avoid using the “save password” feature in your browser, and protect your account against unwanted access on your end (for example, do not share your login credentials with others, or allow them free access to your logged-in device). If you have any questions regarding the security of our Services, please feel free to contact us using the contact information below.

Do We Collect Information from Minors?

Our Services are not intended for persons under 13 years of age. We do not knowingly collect or process the personal information of individuals under the age of 13. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that a child under 13 may have provided us their Personal Information, please contact us at privacy@paymentlabs.io.

What Are Your Privacy Choices?

You can control the collection and use of personal information for some of our processing activities. This includes:

Adjusting Communication Preferences

Email: You may unsubscribe from promotional and other types of communications by following the “unsubscribe” instructions near the bottom of the email. You may also email us using the address listed below. Please note, opting out of promotional emails will not stop you from receiving all emails from the company. For example, we may still send you emails pertaining to your purchases, registrations, consumer surveys and similar transactions.

Text Messages: You may opt out of automated text notifications any time by replying “STOP,” or any alternative keyword we have shared with you.

Mail Promotions: You may ask us to unsubscribe from our mail promotions and solicitations by clicking on “Unsubscribe.”.

Push Notifications: You may opt out any time by adjusting your device or app settings or uninstalling our App(s).

Blocking Cookies

Most web browsers automatically accept cookies by default, but you can alter how your browser responds to cookies by adjusting the settings. Information about managing cookies for popular web browsers can be found in the links below:

[Safari](#) (Desktop) and [Safari Mobile](#) (iOS).

[Firefox](#)

[Chrome](#)

[Microsoft Edge](#)

[Brave](#)

Blocking Google Analytics

Many websites, including ours, employ Google Analytics. To opt out of Google Analytics data collection, follow [these instructions from Google](#).

Mobile Device Privacy Settings.

Mobile devices can use device-level information to serve targeted ads. To learn about your privacy choices for your mobile devices, visit these informational pages from [Google \(Android\)](#) and [Apple \(iOS\)](#).

Declining to Submit Personal Information or Requesting its Deletion

If you decline to submit, or request the deletion of, any of your personal information or any portion thereof, you may experience materially reduced Services quality, may be unable to use portions of the Services, or may not be able to use the Services at all. However, you acknowledge and agree that any resulting inability to use the Services or degradation thereof shall not be grounds for any claim of breach, damages, or other liability; nor shall it in any way relieve you of your obligations to Payment Labs. For the avoidance of doubt, the foregoing shall apply whether or not the deletion of personal information or a portion thereof is the result of the exercise of rights afforded pursuant to applicable privacy laws.

International Data Transfers

If you provide personal information through the Websites or Apps, you understand that we may process, store, and transfer your personal information in and to a foreign country, including the United States and hereby consent to such processing, storage, and transfer. The laws that apply to the use and protection of personal information in the United States, or other countries or jurisdictions in which we transfer or process personal information, may be different from the laws and protections in your country. Whenever we engage a service provider, we require that its privacy and security standards adhere to this policy and applicable privacy laws.

Where personal information is transferred from the European Economic Area or the United Kingdom to countries that do not benefit from an adequacy decision, Payment Labs relies on Standard Contractual Clauses approved by the European Commission (Module 2: Controller-to-Processor, and Module 1: Controller-to-Controller as applicable) and the UK International Data Transfer Agreement or UK Addendum, as applicable. Copies of the applicable transfer mechanisms may be requested by contacting privacy@paymentlabs.io.

Non-Personal Information

We may collect information that in and of itself does not permit direct association with any specific person. Such information, and personal information that has been made anonymous or aggregated so that it can no longer be used to identify a specific person is considered non-personal information. In the case of non-personal information we have the right to collect, transfer, use, and disclose this information for any purpose.

Do We Update Our Privacy Policy?

We may update this Privacy Policy from time to time. If we make changes, we will notify you by revising the date at the top of the Policy and, in some cases, we may provide you with additional notice (such as adding a statement to our website homepage or sending you a notification). We encourage you to review the Privacy Policy whenever you access the Services or otherwise interact with us to stay informed about our information practices and the choices available to you.

How Can You Contact Us?

To ask questions or comment about this privacy policy and our privacy practices, contact us at:

Payment Pro Logistics, LLC
14403 Tiara Street, Unit 8
Van Nuys, CA 91401
privacy@paymentlabs.io
1-833-457-5227

SUPPLEMENTAL NOTICES FOR SPECIFIC JURISDICTIONS

Supplemental Notice to Canadian Data Subjects

Canadian laws provide specific rights to our Users who reside in Canada. If you are a Canadian resident, this section applies to you.

We are committed to openness and accountability with respect to how we handle your personal information pursuant to Canadian federal and provincial privacy laws (“Canadian Privacy Law”), including:

- The Personal Information Protection and Electronic Documents Act (PIPEDA)
- Alberta’s Personal Information Protection Act (Alberta PIPA)
- British Columbia’s Personal Information Protection Act (BC PIPA)
- Québec's Act respecting the protection of personal information in the private sector (Québec Act).

Consent. In most cases, we rely on implied consent to collect, use, or disclose your personal information. In some circumstances, including those involving sensitive personal information, we obtain express consent. Where you have provided your consent to the collection, use, and transfer of your personal information (whether orally, in writing, or electronically), you may have the legal right to withdraw your consent under certain circumstances. In addition to the methods described above with respect to your privacy choices, you may withdraw your consent by contacting us at privacy@paymentlabs.io. Please note that if you withdraw your consent, we may not be able to provide you with a particular product or service. We will explain the impact to you at the time to help you with your decision.

Use of Your Personal Information. We will not collect, use, or disclose personal information except for the purposes identified above (*see Disclosures of Your Personal Information*) unless we have received additional consent or the processing is authorized without consent. Where we engage service providers who utilize the personal information we provide to them, we ensure that an agreement is place with them that ensures their compliance with applicable Canadian Privacy Law.

Canadian Access and Challenge Rights. Canadian Privacy Law provides the right to receive information about the existence, use, and disclosure of your personal information and be provided access to that information. You may also challenge the accuracy and completeness of your personal information and have it amended as appropriate. Depending on the nature of the challenged information, amendment may involve correction, deletion, or addition of information.

Exercising Your Canadian Privacy Rights. If you have an account with us, you may view and update your account information (as noted above) directly by logging into your account. To submit a request for access to information not contained within your account, or to challenge the accuracy or completeness of your personal information, you may email privacy@paymentlabs.io or call [+1-833-457-5227](tel:+1-833-457-5227). When submitting a request, we may require

that you take additional steps to validate your identity or legal authority. We will begin processing your request once you have completed the verification process.

We have put procedures in place to receive and respond to inquiries about our policies and practices relating to the handling of personal information. We will provide a response to any personal information request within the timeframe required by law. If we cannot substantively respond to your request in a timely manner, we will notify you and state the reason for the delay. Under certain circumstances, we may not be able to fulfill your request, such as when doing so would interfere with our regulatory or legal obligations, where we cannot verify your identity, or if your request involves disproportionate cost or effort. However, we will respond to your request within a reasonable time, as required by law, and provide an explanation.

Additional information about how to exercise your rights under Canadian Privacy Law can be found here:

Office of the Privacy Commissioner of Canada

[Website](#)

Toll-free: 1-800-282-1376

Office of the Information and Privacy Commissioner of Alberta

[Website](#)

Toll-Free: 1-888-878-4044

Edmonton office: (780) 422-6860

Calgary office: (403) 297-2728

Office of the Information and Privacy Commissioner of British Columbia

[Website](#)

Vancouver: (604) 660-2421

Elsewhere in BC: (800) 663-7867

Commission d'accès à l'information du Québec

[Website](#)

Toll-free: 1-888-528-7741

Supplemental Notices for Residents of Certain U.S. States

The rights described below apply to you only if you are a resident of a state within the United States that has an applicable and effective privacy law providing for the below rights:

- **Data portability:** You can ask for a downloadable copy of your personal information in a machine-readable format. You can also request that we transmit the data to someone else where it's technically possible.
- **Knowledge and access:** You may have the right to know more about personal information that we have collected and disclosed in the preceding 12 months. You may be able to access, receive details on collection, the purpose of processing, and any sharing that may have occurred.

- **Deletion:** You have the right to request Payment Labs to delete the personal information we have collected about you under certain circumstances.
- **Non-discrimination for the exercise of your privacy rights:** You have the right to not receive discriminatory treatment by Payment Labs for the exercise of your privacy rights.
- **Rectification:** If you believe that any personal information we are holding about you is incorrect or incomplete, you can request that we change, correct, or supplement the data. You can also correct some of this information directly by logging into your account, if you are a customer. Please contact us as soon as possible if you notice any inaccuracy or incompleteness.
- **Opt-out of sharing your personal information for cross-context behavioral or targeted advertising:** You have the right to request Payment Labs to stop sharing your personal information for the purposes of cross-context behavioral advertising or targeted advertising.
- **No Automated Decision Making:** We do not use any decision making based solely on automated processing, including profiling.
- **Object to Processing:** You may object to the processing of your personal information, or ask us to restrict the processing of your personal information.
- **Opt-Out of Marketing Communications:** You have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing emails we send you.
- **Withdraw Consent:** Similarly, if we have collected and process your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.
- **Right to File a Complaint with a DPA:** You have the right to complain to a data protection authority about our collection and use of your personal information. For more information, please contact your local data protection authority.

Targeted Advertising

We engage in targeted advertising which means we display ads to our users based on personal information obtained from their activities over time and across nonaffiliated websites and apps. This allows us to serve you more relevant ads that align with your preferences and interests. We feel this creates a more pleasurable experience for our users. However, if you decide you want to opt out of sharing your personal information for targeted advertising purposes, you can opt out (*see Exercising Your Rights* below). Please note, opting out of targeted advertising does not mean that you will no longer receive ads from us—it just means that such ads will not be specifically tailored to you.

Sale of Personal Information.

“Selling” means the exchange of personal information to third parties in exchange for money or other remuneration. We do not sell your personal information to third parties.

Exercising Your Rights. Please send requests exercising the above rights to our privacy team at privacy@paymentlabs.io.

We will verify your request using your name and email. Depending on the nature of your request, we may need additional information to verify your identity. You may authorize an agent to make a request on your behalf to exercise your privacy rights under applicable California privacy laws. If you are a Colorado resident, you may have the right to appeal Payment Labs' denial of an individual rights request. In order to eliminate fraudulent requests and to protect your personal information, we will not accept correspondence via any third-party applications and/or autogenerated template requests emailed to us.

For requests under the CCPA, only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information.

You may only make such a request for access or data portability twice within a 12-month period. The verifiable consumer request must provide sufficient information that allows us to reasonably verify you have had any connection to our services, you are the person about whom we collected personal information while using our services, or that you are an authorized representative making these representations on a consumer's behalf. As it is important to guard against fraudulent claims and protect personal information, we require that your request provides us with sufficient detail to allow us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm that the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. For Data Subjects located in the EEA or UK exercising rights under the GDPR, we will respond within thirty (30) days of receipt of a verifiable request, with a possible extension of an additional sixty (60) days where necessary, consistent with GDPR Article 12(3). We will deliver our written response electronically or in writing if deemed appropriate by our legal counsel. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily usable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Supplemental Notice for European and UK Data Subjects

To the extent that you are a user that resides in the EU or the UK, the terms of this section apply to the collection, storage, and use of your personal information. Under the EU and UK General Data Protection Regulation, or GDPR, EU and UK residents have certain rights regarding their data, including:

- Right to access the personal information;
- Right to correct incorrect personal information that Payment Labs has about you;
- Right to prevent Payment Labs from using your personal information and/or objecting to processing;

- Restricting use of your personal information for use for particular purposes;
- Right to be forgotten (by requesting that Payment Labs delete all of the personal information it has about you); and
- Right to not be subject to automated decision making.

You may make any requests allowed per this section by using the contact information below:

ATTN: Privacy Officer
Payment Pro Logistics, LLC
14403 Tiara Street, Unit 8
Van Nuys, CA 91401
privacy@paymentlabs.io
1-833-457-5227

Definitions.

“Process”, “Processing”, or “Processed” means anything that is done with any of your Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Payment Labs Processes your Personal Information rather than utilizing a third-party processor to do so on our behalf.

“Controller” means the entity that decides how and why Personal Information is Processed. Accordingly, Payment Labs is the Controller of your Personal Information in that we decide how and why your Personal Information is Processed.

“Sensitive Personal Data” means Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, any actual or alleged criminal offenses or penalties, national identification number (as applicable in the EU or UK) or any other information that may be deemed to be sensitive under applicable law.

Grounds for Processing. The GDPR requires that companies processing the personal data of EU and UK users do so on the basis of specific legal grounds. As described below, Payment Labs processes the information of EU and UK users based on one or more of the following grounds as allowed under the GDPR:

- *The processing is necessary to provide the services and features you request.* Payment Labs must collect and use certain information in order to provide its services.

This includes:

User profile information that is necessary to establish and maintain your account, including to verify your identity; enable communications with you about the services you obtain from us, orders and accounts; and to enable you to use the services.

Usage information, which is necessary to maintain, optimize and enhance Payment Labs' services.

- *The processing is necessary to protect the vital interests of our users or of others.* Payment Labs may process personal information, including disclosing data with law enforcement authorities in case of threats to the safety of users or of others.

- *The processing is necessary for Payment Labs' legitimate interests.*

Payment Labs collects and uses personal information to the extent necessary for its legitimate interests. This includes, but is not limited to, collecting and using information:

- To prevent, detect and combat fraud in connection with the use of our services.
- To inform law enforcement officials regarding criminal acts or threats to public safety.
- To provide customer support.
- To optimize our service and develop new services.
- For direct marketing purposes. This includes, for example, analyzing data to identify trends and tailor marketing messages to user needs.
- To enforce Payment Labs' Terms of Service or to protect its interests.

- *The processing is necessary for the legitimate interests of other persons or parties.*

- Payment Labs collects and uses personal information to the extent necessary for the interests of other persons or the general public. This includes sharing information in connection with legal or insurance claims, to protect the rights and safety of others.
- Payment Labs may also process personal information when necessary in regard to a substantial public interest, on the basis of applicable laws

- *The processing is necessary to fulfill Payment Labs' legal obligations.*
- Payment Labs is subject to legal requirements in the jurisdictions in which it operates that require us to collect, process, disclose and retain your personal data. For example, Payment Labs is subject to laws and regulations in many cities and countries that require it to collect and retain information about the Payment Labs services, to retain such information for extended periods of time, and to provide copies of such information to governmental or other authorities. Payment Labs uses your information to comply with such laws to the extent they apply to your use of the Payment Labs services.