



FASTBOY PAYMENTS PRIVACY POLICY

Last Updated: July 1, 2026

Fastboy Payments, LLC (“**Fastboy**,” “**we**,” “**us**,” or “**our**”) provides payment gateway technology and related services. This Privacy Policy explains how we collect, use, disclose, and protect personal information when you use our website, products, and services (collectively, the “**Services**”).

1. Scope of This Privacy Policy

This Privacy Policy applies to personal information processed by Fastboy in connection with:

- our payment gateway platform
- merchant dashboards and developer tools
- application programming interfaces (APIs) and payment integrations
- tokenization and payment credential services
- our websites and documentation portals
- communications with merchants, partners, and users

Fastboy provides technology that enables merchants and partners to securely transmit, route, and manage payment-related data between their systems and payment ecosystem participants (such as payment processors, acquiring banks, and payment networks).

Fastboy does not act as a merchant of record, payment facilitator, acquiring institution, or settlement provider, and does not perform authorization, clearing, or settlement of payment transactions.

This Privacy Policy describes how Fastboy handles personal information when individuals interact with our Services or when information is submitted through merchant or partner integrations.

This Privacy Policy does not apply to third parties (such as merchants, payment processors, financial institutions, or other service providers), which have their own privacy practices.

This Privacy Policy is intended to comply with applicable privacy and data protection laws governing the jurisdictions in which Fastboy provides the Services, including, where applicable, the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), other applicable U.S. state privacy laws, the European Union General Data Protection Regulation (GDPR), and the United Kingdom General Data Protection Regulation (UK GDPR). If Fastboy expands its operations into additional jurisdictions, this Privacy Policy may be updated to reflect applicable legal requirements.

2. Roles and Responsibilities

Merchants and Platforms

Merchants, platforms, and partners using the Services determine what personal information is collected and how it is used in connection with transactions. They are responsible for their own privacy practices and for compliance with applicable data protection laws. Merchants retain control over and responsibility for personal information they collect from their customers.

Fastboy

Fastboy processes personal information as necessary to provide and operate the Services, including transmitting payment-related data and supporting merchant integrations.

In most cases, Fastboy acts as a **data processor** (and “service provider” under the California Consumer Privacy Act) on behalf of merchants. In limited circumstances, Fastboy may act as a **data controller** where required to comply with legal obligations, enforce agreements, or protect the security and integrity of the Services.

Fastboy processes personal information only on documented instructions from merchants except where otherwise required by applicable law.

3. Personal Information We Collect

We collect and process only the minimum personal information necessary to provide and operate the Services.

For purposes of the California Consumer Privacy Act (CCPA), the categories of personal information we collect may include identifiers, commercial information, internet or network activity, and other information described below.

A. Transaction and Payment Information

- truncated or masked payment card numbers
- tokenized payment credentials
- transaction identifiers and metadata
- payment method details
- timestamps and authorization data

Fastboy may store encrypted Primary Account Numbers (PANs) only as necessary to provide the Services and fulfill applicable contractual, legal, regulatory, and payment industry requirements. Full PANs are protected in accordance with PCI DSS requirements and applicable payment industry standards using administrative, technical, and physical safeguards designed to protect payment card data.

B. Device and Technical Information

- IP address
- browser type and device information
- operating system
- API request and system logs
- network and routing data
- device location information (including approximate or precise geolocation, and geofencing data, where enabled on payment devices)

C. Account and Business Information

- merchant contact information
- account credentials and user profiles
- billing and support information
- communications with Fastboy

D. Website Usage Information

- pages visited and interactions
- referral URLs
- analytics data
- cookies and similar technologies

4. How We Use Personal Information

We process personal information only for the purposes described in this Privacy Policy and not in a manner incompatible with those purposes. We do not process personal information for purposes that are materially different, unrelated, or incompatible with the purposes described below.

We use personal information to:

- provide, operate, maintain, and support the Services;
- transmit and process transaction-related data;
- support integrations, APIs, merchant dashboards, and developer tools;
- monitor the performance, availability, and security of the Services;
- detect, prevent, investigate, and respond to fraud, misuse, security incidents, and other unlawful or unauthorized activity;
- maintain system integrity and comply with applicable contractual, legal, regulatory, payment network, and financial institution requirements;
- determine transaction attributes necessary to support applicable payment network, legal, and regulatory requirements (such as location-based surcharging compliance), including the use of geolocation and geofencing controls on payment devices;
- communicate with merchants, partners, and users regarding the Services; and
- comply with applicable legal and regulatory obligations.

Fastboy processes personal information on behalf of merchants and does not retain, use, or disclose such information for any purpose other than providing the Services, except as permitted or required by applicable law.

Fastboy does not use personal information for its own independent marketing purposes. Use of personal information is limited to operating, maintaining, securing, and improving the Services and is not used to profile end users or build independent datasets unrelated to the Services.

We may use aggregated or de-identified information that does not identify individuals for analytics, reporting, and service improvement purposes.

Artificial Intelligence

Fastboy does not use personal information, payment card data, or merchant data processed on behalf of merchants to train publicly available or third-party artificial intelligence or machine learning models. Any use of artificial intelligence technologies by Fastboy is limited to supporting the security, operation, maintenance, and improvement of the Services in accordance with applicable contractual, legal, regulatory, and payment industry requirements.

Sensitive Personal Information

We may process Sensitive Personal Information, including precise geolocation and geofencing data from payment devices, solely as necessary to provide the Services, including transaction processing, determining transaction attributes necessary to support applicable payment network and regulatory requirements, maintaining system security, enforcing device-level controls, and complying with applicable legal and payment network requirements.

Fastboy uses Sensitive Personal Information only for purposes permitted by applicable law, including California Civil Code Section 1798.121.

Location and geofencing data are used only in connection with transaction processing and device-level controls and are not used for behavioral tracking, marketing, or profiling of individuals outside the context of the Services.

Legal Basis for Processing (where applicable)

We process personal information based on contractual necessity, legal obligations, legitimate interests (such as fraud prevention and service security), and, where applicable, user consent.

We do not sell personal information or share personal information for cross-context behavioral advertising.

5. How We Share Personal Information

We may share personal information in the following ways:

With Payment Ecosystem Participants

To enable transactions, information may be shared with:

- payment processors
- acquiring banks
- payment networks
- financial institutions

This may include sharing information for transaction processing, fraud prevention, risk management, and compliance with payment network and financial institution requirements.

With Service Providers

We use third-party vendors to support our Services, such as:

- cloud and infrastructure providers
- security and monitoring vendors
- analytics providers

These providers are contractually required to protect personal information.

Service providers are authorized to process personal information only as necessary to perform services on Fastboy's behalf and are not permitted to retain, use, or disclose such information for any other purpose, except as required by law.

A list of key service providers (subprocessors) may be made available upon request, subject to confidentiality obligations.

With Merchants and Partners

Information may be made available to merchants or partners through dashboards, APIs, or reports.

Business Transfers

In connection with a merger, acquisition, financing, or sale of assets, personal information may be transferred as part of that transaction.

For Legal Reasons

We may disclose personal information where we reasonably believe such disclosure is necessary to:

- comply with applicable law, regulation, legal process, or enforceable governmental requests;
- respond to valid subpoenas, court orders, warrants, or other lawful requests from public authorities;
- protect the rights, property, safety, or security of Fastboy, our merchants, users, or others;
- detect, investigate, prevent, or address fraud, security incidents, or other illegal activity; or
- enforce our agreements or otherwise establish, exercise, or defend legal claims.

Where appropriate and not prohibited by law, Fastboy reviews requests from law enforcement and governmental authorities to confirm they are legally valid before disclosing personal information.

6. Data Retention

We retain personal information for as long as necessary to:

- provide the Services;
- maintain system functionality and logs;
- comply with legal and regulatory obligations; and
- resolve disputes and enforce agreements.

Retention periods are determined based on the purposes for which the data is processed, the nature of the data, applicable legal obligations, contractual requirements, payment network requirements, accounting requirements, fraud prevention needs, security requirements, and risk management considerations.

Certain transaction-related data may be retained in accordance with applicable legal, regulatory, contractual, payment network, accounting, fraud prevention, and security requirements.

Upon termination of the Services, personal information may be securely deleted or retained as required by applicable law, contractual obligations, or legitimate business purposes, in accordance with Fastboy's data retention and secure deletion practices.

7. Data Security

We implement administrative, technical, and physical safeguards designed to protect personal information, including:

- encryption in transit
- access controls
- monitoring and logging
- security testing and maintenance

We maintain incident response procedures and will provide notifications as required by applicable law.

No system is completely secure, and we cannot guarantee absolute security. Users are responsible for protecting their own credentials and systems.

For security-related inquiries, including suspected security incidents, vulnerabilities, or other security concerns, please contact us using the Security-Related Matters contact information listed in Section 14.

8. International Data Transfers

We may process and store personal information in the United States and other countries where we or our service providers operate.

Data protection laws in these jurisdictions may differ from those in your country of residence.

Where required, we implement appropriate safeguards, including Standard Contractual Clauses or other legally recognized transfer mechanisms.

These provisions apply to transfers involving the European Economic Area (EEA), United Kingdom (including UK GDPR requirements), and other jurisdictions with data transfer requirements.

9. Your Privacy Rights

Depending on your location, you may have rights to:

- access personal information
- correct inaccurate data
- request deletion

- restrict or object to processing
- request data portability

Where processing is based on consent, individuals have the right to withdraw consent at any time, without affecting the lawfulness of processing prior to withdrawal.

We may take reasonable steps to verify the identity of individuals, including requesting additional information where necessary, before processing privacy requests.

Privacy requests may be submitted in a format accessible to the individual.

U.S. State Privacy Rights

Residents of certain U.S. states, including California, Virginia, Colorado, Utah, and Texas, may have additional privacy rights under applicable laws, including the right to appeal decisions regarding privacy requests.

To submit an appeal, please contact us using the information below. We will review and respond within the timeframe required by applicable law.

California Privacy Rights (CCPA/CPRA)

California residents have the right to:

- request disclosure of the categories and specific pieces of personal information collected
- request disclosure of categories of personal information disclosed to third parties for business purposes
- request deletion of personal information
- request correction of inaccurate information
- limit the use of sensitive personal information (where applicable)

California residents may designate an authorized agent to make requests on their behalf, subject to verification requirements.

We will not discriminate against individuals for exercising their privacy rights.

European Economic Area and United Kingdom (GDPR)

Individuals in the EEA and UK have the right to lodge a complaint with a supervisory authority.

Fastboy does not engage in solely automated decision-making or profiling that produces legal or similarly significant effects on individuals. Fastboy may use automated systems to support fraud detection, security monitoring, transaction integrity, and operational functions. These systems assist in providing the Services and do not independently make decisions that produce legal or similarly significant effects on individuals without appropriate human oversight where required by applicable law.

Fastboy does not currently designate a Data Protection Officer unless required by applicable law.

If your information was provided through a merchant, you should contact that merchant directly. We will assist as required by law.

To submit a request, contact: privacy@fastboypay.net

10. Children's Privacy

The Services are intended for businesses and their authorized personnel and are not directed to children under the age of 13. Fastboy does not knowingly collect personal information directly from children under the age of 13 in connection with the Services.

If we become aware that we have collected personal information directly from a child under the age of 13 in violation of applicable law, we will take reasonable steps to delete the information or otherwise comply with applicable legal requirements.

Parents or legal guardians who believe that a child under the age of 13 has provided personal information to Fastboy may contact us using the contact information provided in Section 14.

11. Cookies and Tracking Technologies

We use cookies and similar technologies to:

- operate and secure the website;
- analyze usage and performance; and
- improve user experience.

Our website uses Google Analytics to help us understand how visitors interact with our website and to improve website performance and usability. Google Analytics may collect information such as IP address, device information, browser type, pages visited, referring URLs, and interactions with the website.

Where required by law, we obtain consent for non-essential cookies and analytics technologies.

You can manage cookies through your browser settings. You may also be able to manage analytics tracking through tools made available by Google or through applicable consent preferences provided on our website.

Our Services do not currently respond to “Do Not Track” signals.

12. Third-Party Services

Our Services may integrate with third-party platforms or applications. We are not responsible for the privacy practices, security, or compliance obligations of those third parties.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Updates will be posted on this page with a revised “Last Updated” date.

14. Contact Us

If you have questions about this Privacy Policy or wish to exercise your privacy rights, please contact us using the appropriate contact information below.

Privacy Requests

Fastboy Payments, LLC
Attn: Privacy Team
11011 Richmond Ave., Suite 900
Houston, Texas 77042
Email: privacy@fastboypay.net

Security-Related Matters

To report a suspected security incident, vulnerability, or other security concern, please contact:
Email: security@fastboypay.net

Legal Requests

For subpoenas, court orders, warrants, or other legal requests, please contact:
Email: legal@fastboypay.net