PRIVACY NOTICE

Effective Date: April 10, 2026

This Privacy Notice describes how Rainforest Pay, Inc. ("Rainforest," "we," "us," or "our") collects, uses, discloses, and retains information in connection with (i) our website(s), (ii) our payment processing and related services provided to software platforms and merchants (the "Services"), and (iii) our business operations (including onboarding, underwriting, risk management, and compliance screening).

Rainforest is a white-labeled payments infrastructure provider. In most cases, end customers buying goods or services ("End Customers") interact with the merchant or software platform they are transacting with, not directly with Rainforest. However, Rainforest receives and processes End Customer information as part of enabling, protecting, and overseeing payment transactions, including through Rainforest-hosted payment components that may be embedded in a platform's or merchant's checkout experience.

1. Scope

This Notice applies to the following categories of individuals:

- **Website Users:** visitors to our website(s) and individuals who contact us directly;
- **Business Users:** representatives of current, prospective, or former Platforms and Merchants, including administrators, authorized users, and beneficial owners;
- **End Customers:** individuals whose information is processed in connection with a transaction or attempted transaction through our Services; and

Important for End Customers: If you are an End Customer, please also review the privacy notice of the merchant and/or software platform through which you are transacting. They are typically the primary point of contact for privacy requests and disclosures regarding your transaction. PayPal, Inc. is an independent data controller with respect to the processing of your Personal Data in connection with certain payment services. For more information about how PayPal processes your data, please see the PayPal Privacy Statement at https://www.paypal.com/legalhub/privacy-full.

2. Information We Collect

The information we collect depends on the nature of the interaction and the Services being provided. The categories below are illustrative and may overlap.

2.1 Information You or a Platform/Merchant Provide

We may collect information provided directly by you, or provided to us by Platforms and Merchants on your behalf, including:

- Identifiers and contact details (e.g., name, email address, phone number, billing and shipping address);
- Business information for Platforms and Merchants (e.g., company name, DBA name, business address, entity formation information, beneficial owner and representative information, ownership percentages);
- Identity verification information (e.g., date of birth, government identifiers such as SSN/EIN, identity document verification results);
- Payment and transaction information (e.g., transaction amount, transaction identifiers, payment method type, card BIN/last4/card hash/brand/expiry, bank routing and account numbers, wallet identifiers/tokens, MCC, item details); and
- Communications and support information (e.g., support ticket content, emails, chat messages).

2.2 Information Collected Automatically

When you interact with our website, portal, or Rainforest-hosted payment components (such as embeddable checkout fields), we and our service providers may automatically collect:

- IP address and approximate location derived from IP;
- Device identifiers, session identifiers, browser type, operating system, and user agent;
- Language and time zone;
- Log and usage data relating to interactions with our Services; and
- Device intelligence and behavioral biometrics collected via third-party SDKs) embedded in Rainforest-hosted payment components for fraud prevention and security. This may include data about how you interact with the payment form (e.g., typing patterns, mouse movements, touch interactions) and device-level signals. This data is collected directly by the SDK and transmitted to the fraud detection vendor; it is not transmitted through Rainforest's servers.

2.3 Information from Third Parties

We may receive information from third parties in connection with the Services, including from Platforms and Merchants, sponsor banks, payment processors, card networks, and specialized fraud/risk/compliance vendors. This may include risk signals and scores, identity verification results, sanctions/PEP screening results, adverse media signals, rule triggers, and transaction-related status or dispute data.

3. How We Use Information

We use information for the following business purposes:

- Provide, operate, and support the Services, including transaction execution, authorization, routing, settlement, reconciliation, customer support, and account administration;
- Detect, prevent, investigate, and remediate fraud, suspicious activity, account misuse, and other security incidents;
- Perform compliance functions, including identity verification (KYC), business verification (KYB), sanctions/PEP screening and monitoring, adverse media monitoring, and anti-money laundering screening;
- Manage disputes, chargebacks, refunds, account updates, and transaction integrity;
- Develop, test, tune, and improve our fraud, risk, and compliance controls and the reliability of our Services, including using transaction-level data across merchants and platforms where appropriate for system integrity and fraud prevention;
- Maintain auditability and comply with legal, regulatory, sponsor bank, and card network obligations (including recordkeeping and tax reporting); and
- Protect our rights and the rights of others, and enforce our agreements.

4. How We Disclose Information

We may disclose information as follows:

- **Platforms and Merchants:** in connection with providing the Services, supporting transactions, and providing reports and reconciliation;
- **Service providers and vendors:** that help us operate the Services, including cloud hosting, customer support tools, and specialized fraud/risk/compliance vendors for fraud detection, risk scoring, device intelligence, KYC/KYB, and sanctions screening;
- **Payment ecosystem participants:** including payment processors, gateways, sponsor banks, and card networks as required to execute and oversee transactions and manage risk;
- **Regulators, law enforcement, and legal process:** where required by law, subpoena, or legal process, or where reasonably necessary to prevent fraud or protect the security and integrity of the Services; and
- **Corporate transactions:** in connection with a merger, acquisition, financing, or sale of assets.
- **Advertising and Marketing***:* We share Visitor Personal Data with third parties so that we can advertise and market our Services. We do not transfer your Personal Data to third parties in exchange for payment, but we may provide your data to third party partners, such as analytics providers, customer relationship management software providers, and advertising partners who assist us in advertising our Services. We (or service providers on our behalf) may send out communications and marketing outreach to your emails or profiles.

- **Data Analytics:** We use third parties to assist us in analyzing data regarding visitors to our website, for advertising, and for lead generation.

Opt-Out

- To opt out of third-party tracking and advertising, please visit the following opt-out links:
- Google Analytics: Download Google's Opt-Out Browser Add-on
- Google Ads: Manage at **https://myadcenter.google.com/personalizationoff**
- Apollo.io: Contacting privacy@apollo.io or visit the Apollo Privacy Center
- LinkedIn: Visit **https://www.linkedin.com/psettings/guest-controls**

5. Cookies and Similar Technologies

We (and our service providers) may use cookies and similar technologies to operate our website and portal, maintain sessions, prevent fraud, and understand usage. You can control cookies through your browser settings; however, disabling cookies may affect functionality.

In addition, the third-party SDK embedded in Rainforest-hosted payment components collects device and behavioral signals directly for fraud prevention purposes. This collection is not cookie-based and is not controllable through browser cookie settings. For more information, see Section 2.2.

Some browsers offer a 'Do Not Track' feature. Because there is not yet a common understanding of how to interpret these signals, we do not currently respond to browser Do Not Track signals. However, we recognize and process Global Privacy Control signals as required by applicable law.

6. Retention

We retain information for as long as necessary to provide the Services and for additional periods as required or permitted by law and applicable payment ecosystem rules. Retention periods vary by data type and purpose:

- **Transaction records and related account data** are generally retained for at least seven (7) years, and longer where required for legal, regulatory, sponsor bank, or card network compliance, dispute handling, and fraud investigation.
- **KYC/KYB and sanctions screening records** are generally retained for at least seven (7) years from termination of the merchant relationship, and longer where required for compliance and auditability.
- **Fraud/risk scores and service request logs** (including vendor response payloads) are currently retained indefinitely for debugging, quality assurance, fraud investigation, and model validation.

- **Device intelligence and behavioral biometrics data** collected by third-party SDKs is retained by the applicable vendor per the vendor's own retention policy; data retained by Rainforest in service logs is subject to the same retention practices as other service request logs.
- **Operational logs** are retained for periods consistent with security, debugging, and audit needs.

Where retention is no longer necessary for the purposes above, we will delete, deidentify, or aggregate information as appropriate, subject to technical feasibility and legal requirements. As of the date of this Notice, we have not yet implemented automated deletion or purging for all data categories, and we are building a data lifecycle program to address this.

7. Security

We maintain reasonable administrative, technical, and physical safeguards designed to protect information, including security controls aligned with payment industry requirements (such as PCI DSS where applicable), encryption in transit and at rest, and key management controls appropriate to the sensitivity of the data. No system can be guaranteed to be 100% secure; however, we take security seriously and design controls appropriate to the sensitivity of the data we process in the payment ecosystem.

8. Your Privacy Choices and Rights

Your rights may vary depending on where you live and the context of our relationship with you. In many cases, Platforms and Merchants are the primary interface with End Customers and may be responsible for responding to End Customer privacy requests. Rainforest will make commercially reasonable efforts to support verified requests as required by law.

8.1 California (CCPA/CPRA) Notices

If you are a California resident, you may have the right to:

- Request access to the categories and specific pieces of personal information we have collected about you;
- Request correction of inaccurate personal information;
- Request deletion of personal information, subject to legal exceptions;
- Opt out of the "sale" or "sharing" of personal information (as defined under the CPRA); and
- Not be discriminated against for exercising these rights.

We do not sell personal information and we do not share personal information for cross-context behavioral advertising. Accordingly, there is no "sale" or "sharing" to opt out of.

Certain information may be exempt from access or deletion under applicable law, including where retention is required for legal compliance, security, fraud prevention, dispute handling, or transaction recordkeeping.

To submit a request, please contact us using the information in Section 11. We may need to verify your identity or your authority to make the request before we can respond.

8.2 Categories of Personal Information Collected

The following table summarizes the categories of personal information we may collect, the purposes of collection, and the categories of third parties to whom we may disclose such information, consistent with CCPA/CPRA requirements:

CCPA Category	Business Purpose	Categories of Recipients
Identifiers (name, email, phone, address, SSN/EIN, DOB)	Transaction processing, KYC/KYB, compliance, fraud prevention, customer support	Platforms, Merchants, service providers, Risk Vendors, sponsor banks, card networks, regulators
Financial information (bank account, routing, card data, transaction details)	Transaction execution, settlement, disputes, fraud detection, compliance	Platforms, Merchants, service providers, Risk Vendors, sponsor banks, card networks, processors
Commercial information (transaction history, items, amounts)	Transaction processing, reconciliation, risk management, reporting	Platforms, Merchants, service providers, Risk Vendors
Internet / electronic activity (IP, device ID, browser, usage logs)	Fraud prevention, security, debugging, service improvement	Service providers, Risk Vendors
Geolocation (approximate, from IP address)	Fraud prevention, compliance	Risk Vendors
Sensory data (behavioral biometrics via SDK)	Fraud prevention and detection	Risk Vendors (collected directly by SDK)
Professional / employment info (business role, title)	Account administration, KYC/KYB	Platforms, service providers
Sensitive personal information (SSN/EIN, financial account credentials, precise	Identity verification, compliance, fraud prevention, transaction processing	Service providers, Risk Vendors, sponsor banks (as required for Services)

geolocation where applicable)		

8.3 Sensitive Personal Information

We may process sensitive personal information (such as government identifiers, financial account information, and device/behavioral signals) where necessary to provide the Services, prevent fraud, verify identity, and comply with law. We do not use sensitive personal information to infer characteristics about you for advertising purposes. We use sensitive personal information only for the purposes expressly permitted under CCPA/CPRA for service providers.

8.4 Other State Privacy Laws

If you are a resident of Colorado, Connecticut, Virginia, Texas, or another state with an applicable consumer privacy law, you may have similar rights to access, correct, delete, and opt out. To exercise any applicable rights, please contact us using the information in Section 11.

8.5 Appeals

Where required by law, you may appeal a decision we make regarding your privacy request. You may submit an appeal by contacting us as described in Section 11 and stating that you are appealing a privacy decision. We will respond within the timeframe required by applicable law.

9. Children

Our Services are not directed to children, and we do not knowingly collect personal information from children under the age of 18. If you are under the age of 18, you may not use the Services.

10. International Users

Rainforest's Services are currently designed for and offered within the United States. If you are located outside the United States and your information is processed in connection with a transaction through the Services, please be aware that your information will be transferred to and processed in the United States.

11. Contact Us

If you have questions about this Privacy Notice or want to submit a privacy request, you may contact us at:

Rainforest Pay, Inc.

Attn: Privacy Team

4062 Peachtree Rd NE STE A-474, Brookhaven, GA 30319-3021

Email: privacy@rainforestpay.com

12. Changes to This Notice

We may update this Privacy Notice from time to time. We will post the updated version on our website with a revised effective date. Material changes may also be communicated through the applicable Services portal or to Platform contacts where appropriate.