

Privacy Policy

Effective date: June 29th, 2026

Last updated: July 26, 2026

Wallet Inc., a Delaware corporation with offices at 275 E. Hillcrest Dr. #160-21, Thousand Oaks, CA 91360 ("Wallet", "us", "we", or "our"), provides a guest-engagement platform that lets businesses offer their customers a personalized, white-label mobile wallet. This Privacy Policy explains how we collect, use, disclose, and protect personal information across the Wallet Properties and our platform.

"Wallet Properties" means our corporate site at <https://wallet.inc>, our application at <https://wall.et>, this legal site at <https://wallet.law>, our developer and news sites (for example <https://wallet.dev> and <https://wallet.blog>), and all other websites, subdomains, and industry or marketing domains that we own or operate (for example our per-industry funnel sites), together with the Wallet platform and related services (collectively, the "Service").

Please read this Privacy Policy together with our Terms and our Cookies Policy. By using the Service, you agree to the collection and use of information as described here.

The two audiences this policy addresses

Wallet serves two distinct groups, and your rights and our role differ depending on which you are:

- Business customers and prospects ("Merchants"). Businesses that subscribe to or evaluate the Service, and the individuals who act on their behalf. For this group, Wallet is the controller of the personal information we collect (for example, account and billing data).
- Guests. The end customers of a Merchant who receive and use the Merchant's white-label wallet. For guest personal information, Wallet generally acts as a service provider or processor on behalf of the Merchant, who is the controller. The Merchant's own privacy notice governs its relationship with its guests; this policy describes what Wallet does with guest information on the Merchant's behalf. See "Our role: controller vs service provider" below.

Definitions

- Personal Information (or Personal Data) means information that identifies, relates to, or could reasonably be linked with a particular individual or household.
- Merchant means a business customer or prospect, as described above.

- Guest means an end customer of a Merchant who uses the Merchant's wallet.
- Usage Data means information collected automatically from your use of the Service or generated by the Service infrastructure (for example, page-visit duration).
- Cookies means small files placed on your device. See our Cookies Policy for detail.

Information we collect

From Merchants (Wallet is the controller):

- Identity and contact data: name, business name, email address, phone number, and business address.
- Account data: login credentials and account settings.
- Billing data: billing contact, plan, and payment details processed through our payment processor (we do not store full card numbers; see "Payments").
- Communications: records of your communications with our sales and support teams.

From Guests (Wallet acts as a service provider or processor for the Merchant):

- Identity and contact data: typically a phone number (the SMS unlock code is sent to it), and any name or contact details the Guest provides to the Merchant.
- Wallet content: passes, offers, points, rewards, tier status, loyalty balance, and "Merchant Credit." A Guest's loyalty balance refers to points, rewards, or perks earned in the Merchant's program. "Merchant Credit" is store credit a Merchant issues to a Guest (for example, as a goodwill credit), redeemable only for that Merchant's own goods or services and never for cash. It cannot be purchased by the Guest, the Service does not currently apply expiration or fees to it, and Wallet holds no funds behind it (we keep the balance record; the Merchant honors it). It is not currency or a financial-account balance.
- Transaction and engagement data: a Guest's interactions with the Merchant's wallet across the lifecycle stages (Visitor, Subscriber, Customer, Member).

From affiliates and partners (Wallet is the controller):

- Affiliate account data: name, email, and account details for individuals or businesses who enroll in our affiliate program at <https://our.wallet.fans>.
- Payout and referral data: payout details and the referral, click, and conversion data used to track commissions, managed through our affiliate platform FirstPromoter.

From all visitors to the Wallet Properties:

- Usage Data and device data: IP address, browser type and version, pages viewed, time and date of visits, time spent on pages, unique device identifiers, and diagnostic data.
- Cookies and similar technologies: as described in our Cookies Policy.

How we use information

We use the information we collect to:

- provide, operate, and maintain the Service;
- create and administer Merchant accounts, process subscriptions, and take payment;
- enable Guests to participate in the interactive features of a Merchant's wallet when they choose to do so;
- administer our affiliate program, including tracking referrals and processing affiliate payouts;
- provide customer support and respond to inquiries;
- send service, transactional, and (where permitted) marketing communications, including SMS messages as described below;
- measure the performance of our marketing and advertising, including by associating your account signup and subscription events (upgrades, downgrades, payments, and cancellations) with the campaign you came from to calculate return on ad spend, using our analytics and advertising accounts (Google Analytics and Google Ads); for this conversion matching we may send Google hashed identifiers (such as a hashed form of your email address or phone number) and coarse location (such as city, region, and postal code);
- analyze and improve the Service, and monitor usage;
- detect, prevent, and address security incidents, fraud, and technical issues; and
- comply with our legal obligations.

SMS and text messaging (TCPA / CTIA)

Text messaging supports the wallet product itself, not our lead-generation funnels. We use SMS in two ways:

- Transactional unlock codes. When a Guest unlocks a Merchant's wallet, we send a one-time passcode to the Guest's phone number. This is a transactional message sent to complete an action the Guest initiated.
- Merchant program messages. A Merchant may send program messages (for example offers or reminders) to its own Guests who have opted in through the Merchant's flow.

The Merchant is responsible for obtaining consent consistent with the Telephone Consumer Protection Act (TCPA) and CTIA guidelines; Wallet provides the messaging platform and processes these messages on the Merchant's behalf.

We do not send SMS marketing to leads or prospects who submit our marketing or lead-magnet forms.

- Opt-out and help. Recipients can text STOP to opt out and HELP for assistance.
- Rates. Message frequency varies; message and data rates may apply.
- Carrier disclaimer. Carriers are not liable for delayed or undelivered messages.
- A2P 10DLC. Messaging is registered and sent in accordance with carrier application-to-person (A2P 10DLC) requirements.
- No third-party sharing of mobile opt-in data. We do not sell, rent, or share mobile phone numbers, SMS opt-in information, or messaging consent with third parties for their own marketing or promotional purposes. We share this information only with the service providers that operate the messaging on our and the Merchant's behalf (for example Twilio) and only to deliver the messages you have opted into.

Cookies and tracking

We use cookies and similar technologies to operate the Service, remember preferences, provide security, and analyze usage. On our marketing and corporate sites we use Google Analytics 4 (GA4), including server-side events sent through Google's Measurement Protocol (for example, account signups, subscription upgrades and downgrades, payments, and cancellations), and we link those GA4 accounts to our Google Ads accounts to associate these events with the advertising campaign a visitor came from and measure our advertising and return on ad spend. We also use the Meta pixel and the LinkedIn pixel to promote and measure our marketing. This advertising measurement is a "sharing" of information you can opt out of, as described in our Cookies Policy and the CCPA/CPRA section below. The separate GA4 property used inside the wallet product is not linked to any advertising account and is not used for advertising.

Merchant analytics inside a wallet. A Merchant may add its own analytics (for example, its own Google Analytics tag) to the wallet it offers its Guests. Where a Merchant does so, that analytics provider receives the Guest's in-wallet activity under the Merchant's own account and configuration; the Merchant is the controller of that data, its own privacy notice applies, and Wallet does not control the Merchant's analytics configuration. Wallet does not use the wallet product's Guest data for its own advertising and does not sell or share it for cross-context behavioral advertising.

Service providers and sub-processors

We engage third parties to perform services on our behalf. They may access personal information only to perform those services and are obligated to protect it. These include, for example:

- Stripe, for subscription and add-on payment processing on Wallet's own account (<https://stripe.com/privacy>);
- Google, for Google Analytics 4 (GA4) website analytics including server-side Measurement Protocol events (service provider), and Google Wallet passes (<https://policies.google.com/privacy>);
- Google Ads, Meta (Facebook/Instagram), and LinkedIn, for advertising and campaign measurement on our marketing websites (this is the cross-context behavioral advertising "sharing" described in our Cookies Policy);
- Amazon Web Services (AWS), for cloud hosting, and Cloudflare R2, for media storage;
- Twilio, for SMS (unlock codes and Merchant program messages) and carrier A2P 10DLC registration;
- Mailgun, for transactional and notification email;
- ActiveCampaign, for email and CRM / marketing automation;
- ChatKitty, for in-wallet public chat rooms (processes guest identifiers and message content);
- ip-api (Artia International S.R.L.), for IP-based geolocation of website visitors;
- Svix, for delivering Merchant webhooks;
- FirstPromoter, for affiliate signups, referral tracking, and commission payouts for our affiliate program at <https://our.wallet.fans>; and
- Slack and Google Sheets / Drive, for internal notifications and marketing operations.

Payments

We use third-party payment processors (for example, Stripe) to process payments. We do not store full payment card details; that information is provided directly to the processor, whose handling of your information is governed by its own privacy policy. Our processors adhere to PCI-DSS standards.

Disclosure of information

We may disclose personal information:

- to comply with a legal obligation, court order, or valid request by a public authority;
- to protect and defend our rights or property, prevent or investigate wrongdoing, protect the safety of users or the public, or protect against legal liability;
- to a Merchant, where the information is Guest information we process on that Merchant's behalf; and
- in connection with a merger, acquisition, financing, or sale of assets, subject to this policy.

We do not sell personal information. Where we use analytics only to understand usage, and our analytics is not linked to any advertising account (as with the GA4 property inside the wallet product), that is a service-provider arrangement, not a sale or share. On our marketing websites, however, our Google Analytics accounts are linked to our Google Ads accounts, and our advertising technologies there (Google Ads, the Google Analytics-to-Google Ads conversion and return-on-ad-spend measurement described above, and the Meta and LinkedIn pixels) may involve the "sharing" of visitor and customer information for cross-context behavioral advertising as that term is defined under California law. You can opt out of this sharing by emailing privacy@wallet.inc; see the CCPA/CPRA section. We are also deploying a "Do Not Sell or Share My Personal Information" control and Global Privacy Control (GPC) support across our websites. We do not sell or share Guest wallet personal information for advertising.

Data retention

We retain personal information for as long as it is needed for the purposes described in this policy, and then delete or de-identify it, unless a longer period is required by law.

- Merchant account data: when a Merchant cancels, the account is placed in a "frozen" state rather than immediately deleted (login and features are disabled and billing stops), so the Merchant can later return. A Merchant may request deletion of its account data by contacting privacy@wallet.inc, and we will honor verified requests as required by applicable law.
- Guest data: retained per our agreement with the relevant Merchant and that Merchant's instructions; on termination, we return or delete it as provided in the Merchant agreement and Data Processing Addendum.

Security and data-breach notification

We use commercially reasonable administrative, technical, and physical safeguards to protect personal information. No method of transmission or storage is completely secure, so we

cannot guarantee absolute security. In the event of a data breach affecting your personal information, we will notify affected individuals and regulators as required by applicable law.

Your privacy rights

California residents (CCPA / CPRA). If you are a California resident, you have the right to:

- know the categories and specific pieces of personal information we collect, use, disclose, and (if applicable) sell or share;
- request deletion of your personal information;
- request correction of inaccurate personal information;
- opt out of the "sale" or "sharing" of personal information and of targeted advertising; and
- limit the use of sensitive personal information.

Categories of personal information we collect may include identifiers, customer records, commercial information, internet or network activity, and geolocation (approximate).

Sensitive personal information. The sensitive personal information we may collect is limited to your account log-in credentials. We do not use sensitive personal information to infer characteristics about you or for purposes that, under California law, would require us to offer a right to limit its use; if that changes, we will provide a "Limit the Use of My Sensitive Personal Information" control. To make a request in the meantime, contact privacy@wallet.inc.

To exercise these rights, including to opt out of the "sale" or "sharing" of your personal information, contact us at privacy@wallet.inc. We are deploying a "Do Not Sell or Share My Personal Information" control and Global Privacy Control (GPC) support across our websites. We will not discriminate against you for exercising your rights. You may use an authorized agent to submit requests, subject to verification.

Do Not Track (CalOPPA). We do not currently respond to "Do Not Track" browser signals.

International users

The Service is currently directed to users in the United States, and we process information in the United States. If you access the Service from outside the United States, you do so on your own initiative.

Our role: controller vs service provider

For Merchant information (account, billing, sales, and support), Wallet is the controller and this policy governs. For Guest information that we process to deliver a Merchant's wallet, Wallet acts as a service provider or processor on the Merchant's behalf, processing that information only on the Merchant's documented instructions and as set out in the Merchant agreement and the Data Processing Addendum. Guests should consult the relevant Merchant's privacy notice for the controller-level disclosures about that Merchant's program.

Children's privacy

The Service is not directed to children under 13, and we do not knowingly collect personal information from children under 13. We do not sell or share the personal information of consumers we know to be under 16 without opt-in consent (from the consumer if 13 to 15, or from a parent or guardian if under 13), as required by California law. Some Merchant programs are age-restricted (for example, alcohol Merchants may require Guests to be 18 or older, and gaming or casino Merchants may require 21 or older). Merchants in those verticals can enable an age gate that screens Guests at entry and redirects anyone under the required age. If you believe a child under 13 has provided us personal information, please contact us and we will take steps to delete it.

Changes to this Privacy Policy

We may update this Privacy Policy from time to time. We will post the updated policy on this page, update the "Last updated" date, and, where appropriate, provide additional notice (for example by email or a prominent notice on the Service) before the change takes effect.

Contact us

Questions about this Privacy Policy or your personal information:

- Email: privacy@wallet.inc
- Mail: Wallet Inc., 275 E. Hillcrest Dr. #160-21, Thousand Oaks, CA 91360