Rebound Credit Inc. Privacy Policy

Version 2.0 · Published August 23, 2026

Rebound Credit Inc. (**Rebound**, **we**, **us**, or **our**) is accountable for personal information under applicable Canadian privacy law, including the Personal Information Protection and Electronic Documents Act and applicable provincial private-sector privacy laws.

This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information through reboundcredit.ca, the Rebound web application, applications, the restricted-purpose credit account, payments, customer support, and monthly Equifax furnishing.

Our Privacy Officer may be contacted at privacy@reboundcredit.ca or at Rebound Credit Inc., Attention: Privacy Officer, 1800 – 330 5 Avenue SW, Calgary, Alberta T2P 0L4.

1. Scope and consent

This Policy is a notice of our practices. Where law requires consent for a specific purpose, Rebound asks for it separately and in a form appropriate to the sensitivity and reasonable expectations involved. Required Terms, electronic-delivery/e-sign consent, credit agreement acceptance, Equifax furnishing consent, scheduled card authorization, and cancellation/refund acknowledgment are recorded separately. Marketing is optional, unchecked by default, and may be withdrawn without affecting the credit account.

We may collect, use, or disclose information without consent where law permits or requires it, including to investigate fraud, collect a debt, respond to a lawful order, protect a person's safety, or complete a business transaction with appropriate safeguards.

You may withdraw consent subject to reasonable notice and legal or contractual restrictions. Before withdrawal takes effect, we will explain material consequences. Withdrawal does not undo processing already lawfully completed, require deletion of accurate credit history, or erase records we must preserve. It may prevent a feature that genuinely requires the information.

2. Information we collect

Login and contact information

We collect email address, password authentication records, preferred first name, legal name, Canadian mobile number, phone-possession verification events, residential address, and communication preferences. Passwords are handled through Supabase authentication and are not available to Rebound staff in readable form.

Application and eligibility information

We collect date of birth, province of residence, address information as entered and normalized, age/province eligibility decisions, application status, correction history, and evidence that required steps were completed. The MVP does not perform identity-document, selfie, liveness, or third-party identity-verification sessions.

Social Insurance Number

If the active application policy requires or requests a Social Insurance Number (**SIN**), the collection screen explains its purpose and whether providing it is required for that application. The browser treats the SIN as write-only: it is not placed in browser storage or read back after submission. Rebound's preferred MVP design transmits the value directly through the configured secure provider path and retains only an opaque receipt, not the full SIN. Any provider retention or use must be limited by contract and disclosed before activation. Rebound never includes a full SIN in analytics, ordinary logs, support views, documents, or customer-visible history.

Service, credit-account, and transaction information

We collect the plan and immutable catalogue version you select; Service price, applicable tax, financed total, credit limit, annual term and installment schedule; account status; posted purchases; ledger entries; balances derived from the ledger; statements; installment and payment status; cancellations; refunds; disputes; chargebacks; closure; and support or correction records.

Payment-card information

Payment-card entry is hosted or tokenized by Zūm Rails. Rebound does not receive or store the full card number or card security code. We may receive and retain a provider token and permitted metadata such as card brand, expiry, last four digits, payment status, settlement, refund, dispute, and provider event identifiers.

Equifax furnishing information

If you separately consent and the account opens, we may furnish matching identifiers and account information to Equifax Canada Co. approximately monthly. This may include name, date of birth, address, an identifier permitted by law and the active policy, account opening and closure dates, credit limit, balance, payment history, past-due or delinquency status, disputes, corrections, and account status. The MVP does not use Equifax to obtain a consumer report or score and does not provide credit monitoring or a customer bureau-data display.

Communications and document evidence

We collect messages with support; delivery, bounce, complaint, and suppression information; and immutable evidence about document presentation and acceptance, including document version and hash, accepted artifact, date and time, locale, flow version, configured evidence fields, delivery evidence, IP-derived security data where permitted, and user agent. An acceptance record is created only by an explicit acceptance action, not merely because a page or email was viewed.

Technical and security information

We collect information reasonably needed to operate and secure the Platform, such as timestamps, request and correlation identifiers, session and authentication events, coarse device class, browser/user-agent details, network and security events, error categories, and audit events. We do not intentionally put passwords, one-time codes, session tokens, full SINs, full card numbers, card security codes, or Metro 2 files into logs or analytics.

Optional marketing and attribution

If you choose marketing, we collect the preference and withdrawal history. After account opening, we may ask how you heard about Rebound. That answer is optional attribution and not a referral program.

3. How we use information

We use personal information only for identified, reasonable purposes, including to:

- create and secure a login and verify control of email and mobile contact methods;
- receive and resume an application, validate information, determine supported-province and age eligibility, prevent fraud, and manage corrections;
- generate, present, accept, deliver, and reproduce exact versioned documents;
- present a server-owned offer and, if all conditions are satisfied, open one restricted-purpose credit account atomically;
- provide the annual Service, create the financed purchase, schedule and collect installments, issue statements and receipts, handle refunds and disputes, reconcile provider events, and close the account;
- furnish accurate monthly tradeline information to Equifax under the separate consent, investigate disputes, make corrections, and report closure;
- communicate required application, security, payment, statement, furnishing, service, support, and legal information;
- comply with legal, regulatory, tax, accounting, audit, recordkeeping, sanctions, and court requirements;
- protect customers, Rebound, providers, and the Platform from fraud, abuse, compromise, and unlawful activity;
- measure service reliability through allow-listed operational events and improve accessibility and usability; and
- send marketing only where you separately choose it and applicable law permits.

We do not sell personal information. We do not use full SINs, payment-card data, private financial records, or customer document text for targeted advertising. We do not use the MVP to obtain credit files or scores, provide credit monitoring, perform IDV, or train a customer-facing artificial-intelligence coach.

4. Service providers and disclosures

We disclose only the information reasonably needed for the provider's defined role, under contractual and security controls. Only providers activated for the applicable environment receive data.

- **Supabase** provides hosted authentication, database, and storage infrastructure. It processes login, application, account, and document records according to Rebound's configuration and access controls.
- **Resend** provides production email delivery and custom SMTP for authentication email. It may process email address, message content, and delivery metadata. Rebound uses separate optional marketing consent and operational suppression controls.
- **Canada Post AddressComplete** provides Canadian address suggestion, autocomplete, and normalization. It may process partial and complete address queries and return normalized address information. Manual entry remains available.
- **Zūm Rails** provides the only MVP payment rail: provider-hosted tokenized credit-card processing. It may process card and payment information needed to tokenize, authorize, settle, refund, reconcile, and handle disputes. Rebound does not use Zūm for IDV, EFT, PAD, bank linking, Interac, wallets, or cash access in the MVP.
- **Equifax Canada Co.** receives information only for monthly tradeline furnishing, matching, maintenance, dispute correction, and closure reporting under the separate furnishing consent and applicable law. Rebound does not use Equifax for a credit pull, score, monitoring, or IDV in the MVP.
- **PostHog** is not connected to the interim MVP publication. If Rebound later enables it, Rebound will first complete the privacy and data-residency decision, update this Policy where required, and configure it to receive only allow-listed pseudonymous operational events. Autocapture, session replay, IP capture, person profiles, and personal or financial fields will remain disabled unless a later disclosed and approved configuration permits them.

We may also disclose information to professional advisers, auditors, insurers, fraud-prevention or security specialists, a payment-card network or issuer, a lawful collection provider, regulators, courts, law enforcement, or a buyer or successor in a business transaction, but only as permitted by law and with appropriate safeguards.

We do not copy production personal information into development or staging. Those environments use synthetic fixtures only.

5. Cross-border processing

Some providers or their subprocessors may process or store information outside your province or outside Canada. Information in another jurisdiction may be accessible to courts, law enforcement, national-security authorities, or regulators under that jurisdiction’s laws. Rebound evaluates provider location, contractual terms, access controls, and data minimization before activation. Contact the Privacy Officer for current information about provider processing locations relevant to your account.

6. Cookies and analytics

The Platform uses essential cookies or similar storage for authentication, security, session continuity, preferences, and basic operation. Rejecting essential storage may prevent the secure application from working.

Non-essential analytics are disabled in the interim publication. Rebound does not use session replay or broad browser autocapture. If optional analytics are later introduced, Rebound will update its consent and Policy practices as required and will continue to exclude sensitive data.

7. Communications

Required authentication, fraud, security, application, account, payment, statement, furnishing, collection, support, and legal messages are service communications. They are not optional marketing.

Marketing email or text requires a separate choice where required by law. You can withdraw a marketing preference through the method in the message or by contacting support. Withdrawal does not affect required service communications or the credit account.

8. Retention and disposal

We keep personal information only as long as reasonably needed for the identified purpose and applicable legal, accounting, limitation-period, audit, fraud-prevention, furnishing, and dispute obligations. Retention varies by record type:

- unsuccessful or expired application records follow the active application and legal-retention schedule;
- full SIN is not retained by Rebound under the preferred provider-direct policy; an opaque receipt and access evidence follow the configured schedule;
- authentication and security events are retained for the period needed to protect accounts and investigate incidents;
- posted ledger entries, issued statements, accepted document versions, acceptance events, audit events, provider inbox events, and bureau snapshots are append-only and retained for the legal and operational period applicable to the account;
- tokenized card metadata, payments, refunds, and disputes are retained for payment, accounting, network, and legal requirements; and
- optional marketing preference history is retained to honour and prove the current choice.

When information is no longer required, Rebound securely deletes, anonymizes, or destroys it. Backups age out under controlled schedules. Legal holds, active disputes, fraud investigations, and regulatory obligations may delay disposal.

9. Safeguards and incidents

Rebound uses safeguards appropriate to sensitivity, including encryption in transit and at rest where appropriate; server-only secrets; role separation; least-privilege authorization and row-level security; multi-factor authentication for administrators; masked customer and support views; append-only evidence; provider webhook verification and replay protection; secure development and secret scanning; monitoring; retention controls; and audit events.

No security method is perfect. If a breach creates a real risk of significant harm or another notification duty, Rebound will investigate, contain, document, notify affected individuals and regulators as required, and take corrective action.

10. Access, correction, and choices

Subject to lawful exceptions, you may ask to:

- learn whether Rebound holds personal information about you and obtain access to it;
- understand how it has been used and to whom it has been disclosed;
- correct inaccurate or incomplete information;
- withdraw a consent or marketing choice, subject to explained limits;

- request an accessible format; or
- raise a concern about Rebound's practices.

We may need to authenticate a request without collecting more information than reasonably necessary. Rebound will not return a full SIN, card number, security code, password, secret, or information that would expose another person or compromise security.

If a name, date of birth, address, account, payment, or furnishing fact changes or is corrected, Rebound uses a controlled correction workflow. We preserve the historical record, supersede or reverse it as appropriate, regenerate affected pre-opening documents, and send downstream corrections where required. Support staff do not silently overwrite accepted or furnished history.

Requests may be sent to privacy@reboundcredit.ca. If you are dissatisfied, you may complain to the Office of the Privacy Commissioner of Canada or the applicable provincial privacy regulator without first completing Rebound's process.

11. Children and age of majority

The paid Service is not directed to a person below the age of majority in their province. Rebound uses date of birth and province to determine eligibility before sensitive later steps. If we learn that information was submitted by an ineligible minor, we will restrict the application and handle the information under the applicable policy and law.

12. Changes to this Policy

We may update this Policy to reflect material changes in law, providers, or practices. We will publish the new version and effective date, give notice and request renewed consent where required, and preserve historical versions connected to prior acceptances. We do not retroactively expand a consent through a policy update.

13. Contact

Privacy Officer
Rebound Credit Inc.
1800 – 330 5 Avenue SW
Calgary, Alberta T2P 0L4
privacy@reboundcredit.ca
support@reboundcredit.ca
https://reboundcredit.ca/privacy