

THIRD-PARTY COLLECTIONS PRIVACY POLICY – INTERVAL RECOVERY SERVICES LLC

Effective Date: August 6, 2026

This Third-Party Collections Privacy Policy (the **Policy**) explains how Interval Recovery Services LLC (**Interval, we, us, or our**) collects, uses, discloses, and retains personal information in connection with third-party collection services, Interval-recovery.com, secure portals, payments, communications, credit reporting, and related services.

Interval's address is 356 S 2000 W, Suite A, Pleasant Grove, Utah 84062. Privacy questions and requests may be submitted to Support@interval-recovery.com.

1. SCOPE AND OUR ROLE

This Policy applies to information about consumers, business debtors, guarantors, representatives, website visitors, portal users, client personnel, and other individuals who interact with Interval's third-party collection services.

Depending on the information and Applicable Law, Interval may act as an independent business or controller, a service provider or processor for a creditor, a debt collector, a data furnisher, or another regulated entity. The original creditor's privacy notice may also apply. Where Interval collects as the creditor's agent or service provider, the creditor's privacy notice generally governs the underlying financial information; where Interval owns or purchases an Account, Interval provides its own notice as required by Applicable Law. This Policy does not replace notices required by the Fair Debt Collection Practices Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, or other laws.

2. INFORMATION WE COLLECT

We may collect the following categories of information:

2.1 Identifiers and Contact Information

Names, aliases, postal addresses, email addresses, telephone numbers, account identifiers, usernames, device identifiers, IP addresses, and similar identifiers.

2.2 Account and Transaction Information

Creditor names, balances, principal, interest, fees, service or transaction dates, invoices, contracts, account statements, payment history, delinquency dates, products or services, settlement history, refunds, credits, disputes, chargebacks, and collection status.

2.3 Payment Information

Payment method, tokenized card or bank information, transaction status, authorization records, recurring-payment instructions, receipts, processor responses, returned payments, and fraud indicators. Complete payment credentials are generally collected and stored by PCI-compliant processors rather than Interval.

2.4 Communications and Preferences

Calls, recordings, transcripts, voicemail, text messages, email, letters, webchat, portal submissions, complaints, language and channel preferences, convenient or inconvenient times and places, consent and opt-out records, and interactions with AI or human representatives.

2.5 Dispute and Compliance Information

Debt-validation requests, supporting documents, identity-theft claims, attorney representation, bankruptcy information, military status, death notices, hardship information, cancellation or service disputes, cease requests, fraud reports, legal correspondence, and regulatory complaints.

2.6 Credit and Commercial Information

Consumer-reporting information, tradeline status, dispute results, commercial credit information, public records, and information used to assess whether an Account is eligible for collection or furnishing.

2.7 Internet and Device Activity

Browser type, operating system, device settings, cookie identifiers, pages viewed, links selected, referring pages, login attempts, approximate location inferred from IP address, session activity, error logs, and security events.

2.8 Professional and Business Information

Employer or business name, job title, business contact details, business ownership, authorized-representative status, and information concerning a commercial Account.

2.9 Sensitive Information

Where necessary and lawful, we may process government identifiers, financial-account information, precise account authentication data, health-related billing information, bankruptcy information, and other data treated as sensitive under Applicable Law. Sensitive information should be submitted only through an Interval-approved secure method.

2.10 Inferences and Derived Information

Account categorization, contact effectiveness, likely communication preferences, fraud or security indicators, workflow recommendations, quality scores, compliance flags, and other inferences derived from the information described above. We do not use voice recordings to identify an individual through biometric matching unless we provide any notice and obtain any consent required by law.

3. SOURCES OF INFORMATION

We may receive information from:

- Original creditors, current creditors, clients, servicers, account owners, and their affiliates.
- Consumers, business debtors, representatives, attorneys, relatives, references, guarantors, co-signers, employers, and other people who contact us.
- Payment processors, banks, card networks, communications providers, identity-verification services, fraud-prevention services, and portal providers.
- Consumer reporting agencies and entities involved in credit disputes.
- Public records, courts, bankruptcy sources, address and telephone databases, skip-tracing services, and other lawful data providers.
- Devices, browsers, cookies, analytics tools, logs, and security technologies.
- Interval AI Corporation, Interval affiliates, attorneys, vendors, and collection partners.

Information obtained from third parties may be inaccurate or incomplete. Contact us if you believe information about you is incorrect.

4. HOW WE USE INFORMATION

We may use personal information to:

- Locate and authenticate Consumers, representatives, and business users.
- Collect and service Accounts, communicate about balances, and respond to inquiries.
- Provide validation information and investigate disputes, identity theft, bankruptcy, attorney representation, hardship, complaints, and service issues.
- Offer, administer, authorize, process, reconcile, reverse, and document payments, settlements, and payment plans.

- Furnish, update, suppress, delete, and investigate information with consumer reporting agencies where permitted.
- Determine communication timing, channel, frequency, language, and compliance restrictions.
- Record or transcribe communications and provide AI or virtual-assistant functionality.
- Operate, maintain, troubleshoot, personalize, secure, and improve websites, portals, communications, and collection workflows.
- Detect and prevent fraud, unauthorized access, abuse, security incidents, money laundering, and other unlawful activity.
- Conduct quality assurance, training, testing, evaluation, analytics, research, and product development.
- Enforce agreements, establish or defend legal claims, conduct audits, and collect amounts owed to Interval.
- Comply with licenses, bonds, laws, court orders, subpoenas, audits, regulatory requests, sanctions, and recordkeeping duties.
- Support corporate governance, financing, insurance, transactions, reorganizations, and business continuity.

5. ARTIFICIAL INTELLIGENCE AND PRODUCT IMPROVEMENT

Interval may use artificial intelligence, machine learning, language models, synthesized speech, transcription, automated decision-support, and open-source models to provide collection and support services.

We may use identifiable communications and Account information where reasonably necessary to service the applicable Account, authenticate users, investigate disputes, provide support, maintain security, meet legal duties, conduct quality review, and evaluate system performance.

To develop and improve our own systems, including how our AI assistants respond and how to improve engagement, accuracy, and service quality, Interval uses deidentified or aggregated information wherever practical. Interval does not use protected health information, or nonpublic personal information received from a financial institution, to train or improve its models or products. Any use of identifiable information for training, testing, evaluation, or product improvement is limited to what is reasonably necessary and compatible with the purpose for which the information was collected. You should not provide health, medical, or other sensitive information unless Interval specifically requests it through a secure method. If any solicitation or an attempt to collect a debt is made from a false party identifying itself as Interval, please report it immediately to support@interval-recovery.com.

Interval may use identifiable information across systems where reasonably necessary for security, compliance, error investigation, safety, service operation, or another lawful business purpose. We do not sell collection information for advertising.

AI may make recommendations or generate communications, but Interval may apply human review, client parameters, legal controls, and escalation processes. AI output can be incomplete or inaccurate.

6. HOW WE DISCLOSE INFORMATION

We may disclose personal information to the following categories of recipients for the purposes described in this Policy:

6.1 Creditors and Account Participants

Original creditors, current creditors, clients, servicers, owners, insurers, guarantors, co-signers, representatives, and others involved in the Account, subject to law.

6.2 Service Providers

Database, hosting, cloud, telephony, messaging, mail, artificial-intelligence, transcription, analytics, error-logging, security, identity-verification, payment, compliance, licensing, auditing, legal, and customer-support providers. Interval engages these providers under contracts that require them to protect personal information, to use it only to perform services for Interval, and not to use it to train their own models. A current list of key service providers is available on request, and providers may change.

6.3 Credit and Collection Participants

Consumer reporting agencies, dispute processors, skip-tracing providers, collection partners, attorneys, law firms, courts, process servers, and other entities involved in lawful collection or enforcement.

6.4 Government and Legal Recipients

Regulators, licensing agencies, law enforcement, courts, bankruptcy trustees, taxing authorities, auditors, and other parties when required or reasonably necessary to comply with law, protect rights, prevent harm, or respond to legal process.

6.5 Corporate Transactions

Interval AI Corporation, affiliates, investors, lenders, insurers, advisors, and actual or potential buyers, successors, or transaction counterparties in connection with financing, diligence, merger, acquisition, reorganization, bankruptcy, or sale of assets, subject to appropriate protections. In a financing, diligence, or transaction context, Interval limits disclosures to deidentified or aggregated information, or to the minimum information reasonably necessary under confidentiality obligations, and does not disclose account-level debt details except as permitted by the Fair Debt Collection Practices Act and other Applicable Law.

6.6 At Your Direction or With Consent

Persons you direct us to contact or whom you authorize to receive information.

We may disclose aggregated or deidentified information that cannot reasonably be linked to an identifiable person, subject to Applicable Law.

7. THIRD-PARTY CONTACTS AND CONFIDENTIALITY

Debt-collection laws restrict disclosure of consumer debts to third parties. When Interval contacts a relative, reference, employer, or other person for lawful location information or another permitted purpose, we limit the information disclosed as required by law. We do not authorize public disclosure of an Account through social media or other public channels.

Please avoid discussing another person's Account unless you are authorized. Interval may request documentation of authority before disclosing Account information.

8. COOKIES, ANALYTICS, AND ONLINE TECHNOLOGIES

We may use cookies, local storage, pixels, session-replay or interaction tools, and similar technologies to operate secure sign-in, remember preferences, measure use, diagnose errors, prevent fraud, and improve Online Services.

Browser settings may block some technologies, but doing so may impair authentication, payments, webchat, or portal features. Where required, we will provide controls for nonessential cookies. Because Interval does not sell or share personal information as those terms are defined by applicable state privacy laws, it is generally not required to process opt-out preference signals; where Applicable Law requires Interval to honor Global Privacy Control or another browser opt-out preference signal, Interval will do so.

We do not use collection information for cross-context behavioral advertising or targeted advertising. Our website may link to third parties whose privacy practices are governed by their own notices.

9. SALE, SHARING, AND TARGETED ADVERTISING

Interval does not sell personal information for money. Interval does not share personal information for cross-context behavioral advertising and does not process collection information for targeted advertising as those terms are defined by applicable state privacy laws.

Disclosures to creditors, processors, credit bureaus, attorneys, service providers, regulators, and transaction counterparties for the purposes described in this Policy are not intended as sales. If our practices change, we will provide notices and choices required by law.

10. CREDIT REPORTING

Where permitted, Interval may furnish Account information to consumer reporting agencies and may receive or investigate disputes. We may report payment, settlement, dispute, status, and balance information. Credit reporting is subject to the Fair Credit Reporting Act, Regulation V, state law, bureau requirements, and Account-specific restrictions.

You may dispute furnished information through the relevant consumer reporting agency or directly with Interval using a legally available method. We will not require a particular proprietary form or attachment when the law does not permit that condition.

11. HEALTH AND FINANCIAL INFORMATION

11.1 Health Information

Collection for a healthcare provider may involve protected health information. Where Interval acts as a business associate under HIPAA, we process protected health information only to perform the collection services under the applicable business associate agreement and HIPAA requirements. Interval does not use protected health information to train or improve its models or products; only information that has been deidentified in accordance with HIPAA is used for those purposes. Clients must not send medical records or detailed treatment information unless Interval approves a secure method and the disclosure is legally authorized.

11.2 Financial Privacy

When Interval receives nonpublic personal information from a financial institution, we may process it as a service provider or other authorized recipient under applicable financial privacy law and the institution's instructions. Interval uses that nonpublic personal information only to carry out the collection or servicing activity for which it was provided and does not repurpose it for unrelated uses. This Policy does not replace a financial institution's privacy notice.

11.3 Payment Security

Payment card and bank information should be entered only through approved secure interfaces. Interval uses PCI-compliant practices and providers as applicable. We may retain transaction tokens, last-four digits, bank name, status, authorization records, and other information needed to administer payments without retaining complete credentials.

12. DATA SECURITY

Interval uses commercially reasonable administrative, technical, and physical safeguards designed to protect personal information. Measures may include encryption in transit and at rest, access controls, authentication, logging, vendor review, incident response, backups, and employee confidentiality obligations. Interval maintains a SOC 2 Type II program and PCI-compliant payment practices or providers, as applicable.

No method of transmission or storage is completely secure. We cannot guarantee that unauthorized access, loss, misuse, or interruption will never occur. If a security incident affecting personal information

occurs, Interval will provide the notifications required by Applicable Law. Notify Support@interval-recovery.com promptly if you believe an Account or communication has been compromised.

13. DATA RETENTION

Interval retains Account, communication, payment, dispute, furnishing, licensing, and compliance records for the period required to meet its legal, licensing, credit-reporting, audit, and recordkeeping obligations: generally at least six (6) years after an Account is closed or the relationship ends and no longer than reasonably necessary for those purposes. Interval may retain information longer when needed for Applicable Law, a legal hold, litigation, audits, licensing, credit reporting, fraud prevention, security, backup integrity, enforcement, or legitimate business records.

Retention periods vary by record type, jurisdiction, legal obligation, and operational need. A deletion request does not require deletion where retention is permitted or required. Backup copies may remain until overwritten under ordinary cycles.

14. YOUR PRIVACY RIGHTS

Depending on your residence, relationship with Interval, and Applicable Law, you may have rights to:

- Confirm whether we process your personal information and obtain access to it.
- Request correction of inaccurate information.
- Request deletion, subject to legal and operational exceptions.
- Obtain a portable copy of certain information.
- Opt out of sale, sharing, targeted advertising, or certain profiling.
- Limit certain uses or disclosures of sensitive personal information.
- Withdraw consent where processing is based on consent.
- Appeal a denial of a privacy request.
- Receive information about categories of data, sources, purposes, and recipients.

These privacy rights are separate from debt-validation and credit-reporting dispute rights. A privacy request does not automatically dispute, cancel, validate, or delete an Account or accurate credit information.

14.1 Submitting a Request

Submit a request to Support@interval-recovery.com. Describe the right you wish to exercise and provide enough information for us to identify the relevant records. Do not email highly sensitive documents unless we provide a secure method. Interval and its staff will never ask you to send direct payments to an individual or pay by gift card.

14.2 Verification

We may verify identity using information already associated with you, such as contact information, Account reference, address, or secure authentication. We may deny or limit a request if we cannot reasonably verify identity, an exemption applies, the request is excessive or fraudulent, or fulfilling it would violate another person's rights or Applicable Law.

14.3 Authorized Agents

Where permitted, an authorized agent may submit a request. We may require proof of authorization and direct identity verification.

14.4 Appeals

If Applicable Law provides an appeal right, reply to our decision or email Support@interval-recovery.com with the subject "Privacy Appeal" and explain the basis for appeal.

14.5 Nondiscrimination

Interval will not unlawfully discriminate against you for exercising a privacy right. Exercising a right may affect functionality when the requested information is necessary for secure access, payments, collection compliance, fraud prevention, or another permitted purpose.

15. CALIFORNIA AND OTHER U.S. STATE DISCLOSURES

For residents of states with comprehensive privacy laws, the categories collected during the preceding twelve months may include identifiers, customer-record information, commercial information, internet activity, professional information, sensitive personal information, audio or electronic information, inferences, and information protected under other laws. The sources, purposes, and recipient categories are described in Sections 3, 4, and 6.

Interval does not sell personal information and does not share it for cross-context behavioral advertising. We use and disclose sensitive personal information to provide collection and payment services, authenticate users, prevent fraud, maintain security, comply with law, and perform other legally permitted purposes. We do not use sensitive information to infer characteristics for advertising.

Some information processed in connection with consumer credit, financial services, healthcare, employment, business-to-business activity, legal claims, or regulated records may be exempt from a state privacy law. We will apply the law that governs the specific information and request.

16. INTERNATIONAL INFORMATION AND RIGHTS

Interval may provide services in the United States and other approved countries. Personal information may be processed in the United States and other locations where Interval or its providers operate. Those locations may have different data-protection laws.

Where applicable law requires, Interval or its client will use an approved transfer mechanism and provide additional notices. Individuals in certain jurisdictions may have rights to object to or restrict processing, complain to a supervisory authority, or request information about transfer safeguards. Contact us to exercise applicable rights.

Interval's lawful bases for processing may include performance of a contract, compliance with legal obligations, legitimate interests in collecting and administering Accounts, establishment or defense of legal claims, consent, and other grounds recognized by Applicable Law.

17. CHILDREN

The Online Services are not directed to children under thirteen (13), and users must be at least eighteen (18). We do not knowingly collect information directly from children through the Online Services. Account records may concern a minor when lawfully supplied by a creditor or representative. Contact us if you believe a child submitted information without authorization.

18. COMMUNICATION SECURITY AND PREFERENCES

Ordinary email and text may be visible to other users of a device or account and may not be secure. Use the secure portal or another approved method for sensitive information. You may communicate channel preferences or opt out of electronic collection messages using the method in the message or by contacting support. Communication preferences do not necessarily stop legally permitted notices or processing needed to maintain Account records.

19. CHANGES TO THIS POLICY

We may update this Policy to reflect legal, operational, vendor, or service changes. The effective date above identifies the current version. We will provide additional notice of material changes when required by law. Prior versions may be retained for compliance.

20. CONTACT US

INTERVAL RECOVERY SERVICES LLC

356 S 2000 W, Suite A

Pleasant Grove, Utah 84062

Support@interval-recovery.com

Interval-recovery.com