PRIVACY NOTICE

Collection, Use, Disclosure, and Retention of Personal Information

JIL SOVEREIGN TECHNOLOGIES, INC.

a Delaware corporation

Effective Date: **[•], 2026** | Version: **1.0**

INTRODUCTION

This Privacy Notice (the "**Notice**") describes how JIL Sovereign Technologies, Inc., a Delaware corporation ("**JIL**", "**Company**", "**we**", "**us**", or "**our**"), collects, uses, discloses, retains, and otherwise processes personal information of individuals ("**you**", "**your**") in connection with the services offered through retail.jilsovereign.com, jilsovereign.com, and related properties operated by JIL (collectively, the "**Services**").

This Notice is incorporated by reference into the Terms of Service and the Permissible Use Policy. Capitalized terms not otherwise defined in this Notice have the meanings ascribed to them in the Terms of Service. In the event of any conflict between this Notice and the Terms of Service as to the subject matter addressed herein, this Notice controls.

This Notice applies to residents of the United States and, to the limited extent described herein, to individuals located outside the United States whose personal information we process. If you are located in the European Economic Area, the United Kingdom, or another jurisdiction whose laws grant you additional privacy rights, please review Article VIII for jurisdiction-specific supplements.

If you do not agree with the practices described in this Notice, you must not access or use the Services. Your access to or use of the Services constitutes acceptance of this Notice.

ARTICLE I
SCOPE AND DEFINITIONS

1.1. Scope

This Notice applies to personal information we collect about: (a) visitors to our websites; (b) registered account holders and their authorized users; (c) prospective customers and leads; (d) individuals submitting disputes under the Permissible Use Policy; (e) recipients of our marketing communications; (f) representatives of our

business customers, partners, and vendors; and (g) individuals who otherwise communicate with us.

1.2. What This Notice Does Not Cover

This Notice does not apply to: (a) information about legal entities (corporations, partnerships, LLCs) other than in their representative capacity; (b) publicly available blockchain data, including public wallet addresses and public transaction records, which are not personal information under our interpretation of applicable U.S. law; (c) information collected by third-party websites, services, or applications that you access through links on our Services; or (d) information processed by the separately-operated entity known as getJil, which licenses certain JIL Sovereign intellectual property but is a distinct legal entity with its own privacy practices.

1.3. Defined Terms

"Personal Information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. Personal Information does not include publicly available information, deidentified or aggregated information, or information excluded from the scope of applicable privacy laws.

"Sensitive Personal Information" means a subset of Personal Information that includes government-issued identifiers, precise geolocation, racial or ethnic origin, religious beliefs, union membership, contents of private communications, genetic or biometric data, health information, sex life or sexual orientation information, and financial account credentials.

"Processing" means any operation performed on Personal Information, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, disclosure, transmission, dissemination, alignment, restriction, erasure, or destruction.

"Service Provider" means a third party that processes Personal Information on behalf of JIL for a business purpose, under a written contract restricting further use of such information.

"Third Party" means a natural or legal person, public authority, agency, or body other than JIL, the individual to whom the Personal Information relates, and JIL's Service Providers.

ARTICLE II
CATEGORIES OF PERSONAL INFORMATION WE COLLECT

2.1. Collection Overview

We collect the categories of Personal Information set forth below. The specific information collected depends on your interactions with the Services, the products you purchase, and the information you voluntarily provide.

2.2. Identifiers and Contact Information

We collect your name, email address, postal address, telephone number, display name, and unique online identifiers such as device identifiers, IP address, and cookie identifiers.

2.3. Authentication and Account Information

We collect login credentials (in hashed form only), multi-factor authentication secrets (encrypted), security questions and answers, recovery codes, session tokens, and access logs. We do not store plaintext passwords at any time.

2.4. Commercial and Transaction Information

We collect records of products and services purchased, considered, or viewed; subscription status and history; checkout session data; invoice records; and billing addresses. Payment card numbers, card verification values, and full primary account numbers are processed and stored by Stripe, our payment processor; we receive only tokenized references, the last four digits of the card, the card brand, and the expiration date.

2.5. Internet and Electronic Activity Information

We collect browsing history and interaction data on our Services, including pages visited, time spent on pages, referring URLs, click-stream data, search queries, and interactions with emails we send. This is collected through cookies, pixels, server logs, and analytics tools.

2.6. Device, Technical, and Geolocation Information

We collect device type, operating system, browser type, browser language, screen resolution, general geolocation (country, region, city) derived from IP address, and technical diagnostic data. We do not collect precise geolocation (GPS coordinates) from the Services.

2.7. Content You Submit

We collect content you voluntarily submit, including wallet addresses and transaction identifiers submitted for Checks; documents uploaded to the Secure Document Vault; labels and annotations you apply to monitored wallets and portfolios; support requests and correspondence with us; disputes submitted under the Permissible Use Policy; and feedback or survey responses.

2.8. Inferences

We generate inferences drawn from the information above to create a profile reflecting your preferences, characteristics, and behaviors, solely for the purpose of operating, improving, and securing the Services.

2.9. Sensitive Personal Information

In the ordinary course, we do not request or deliberately collect Sensitive Personal Information from retail customers. To the extent any such information is contained in documents you upload to the Secure Document Vault or submit in connection with an Evidence product, we process it solely for the purpose of providing the Service you requested and retain it subject to the encryption and access-control measures described herein. We do not use Sensitive Personal Information for profiling or targeted advertising.

2.10. Information We Do Not Collect at Retail

Consistent with the Permissible Use Policy, our retail tier does not collect, derive, correlate, or disclose personally identifiable information of third parties who are the subject of a Check. If you submit a wallet address or transaction identifier for analysis, we return institutional attribution and risk signals only. We do not identify the natural person associated with such addresses at retail.

ARTICLE III
SOURCES OF PERSONAL INFORMATION

3.1. Directly From You

We collect Personal Information directly from you when you create an account, purchase a Service, submit a Check, upload a document, communicate with us, respond to a survey, or otherwise interact with the Services.

3.2. Automatically

We collect Personal Information automatically through cookies, server logs, pixels, analytics tools, fraud detection services, and session replay tools (where applicable and consented to).

3.3. From Service Providers and Business Partners

We receive Personal Information from Service Providers and business partners, including: (a) Stripe, our payment processor; (b) identity verification providers we engage to comply with anti-money-laundering obligations where applicable; (c) anti-fraud providers; (d) email delivery and communications platforms; (e) analytics providers; and (f) cloud infrastructure providers.

3.4. From Public Sources

We may obtain Personal Information from public sources, including government databases, sanctions lists, public business filings, and publicly available records, to the extent necessary to verify identity, comply with regulatory obligations, and enforce our agreements.

ARTICLE IV
PURPOSES FOR WHICH WE USE PERSONAL INFORMATION

We use Personal Information for the following business and commercial purposes:

(a) to provide, operate, and maintain the Services, including authenticating users, processing Checks, storing and retrieving documents from the Secure Document Vault, delivering monitoring alerts, generating evidence bundles, and anchoring attestations on CourtChain;

(b) to process payments, billing, subscriptions, and refunds through Stripe and our internal billing systems;

(c) to send transactional communications, including receipts, alerts, security notifications, product announcements, and service messages;

(d) to provide customer support, respond to inquiries, investigate complaints, and resolve disputes, including disputes submitted under the Permissible Use Policy;

(e) to secure our Services against fraud, abuse, unauthorized access, cyberattacks, and violations of our Terms of Service and Permissible Use Policy, including through automated anomaly detection;

(f) to comply with legal obligations, including tax, accounting, recordkeeping, anti-money-laundering, sanctions, subpoena, court order, and regulatory reporting requirements;

(g) to enforce our legal rights, defend against legal claims, and protect the rights, property, and safety of JIL, our customers, and the public;

(h) to improve, test, and develop the Services, including through analytics, A/B testing, and research using deidentified and aggregated data;

(i) to personalize the Services, such as remembering your preferences, suggesting relevant products, and tailoring the user interface;

(j) to send marketing communications about our products and services, subject to your opt-out rights described herein;

(k) to conduct business planning, financial reporting, auditing, and corporate governance activities;

(l) to effect corporate transactions, including mergers, acquisitions, financings, reorganizations, bankruptcies, and asset sales, in which event Personal Information may be transferred to the acquiring or successor entity subject to reasonable protections; and

(m) for any other purpose for which we provide specific notice at the time of collection, or for which you provide consent.

ARTICLE V
HOW WE DISCLOSE PERSONAL INFORMATION

5.1. We Do Not Sell Personal Information

JIL does not and has not sold Personal Information as the term "sell" is defined under the California Consumer Privacy Act, the California Privacy Rights Act, or analogous state laws. JIL does not share Personal Information for cross-context behavioral advertising.

5.2. Disclosures to Service Providers

We disclose Personal Information to Service Providers that assist us in operating the Services. Service Providers are contractually restricted to processing Personal Information only for the purposes for which we engage them and are prohibited from selling or otherwise using such information for their own purposes. Our principal categories of Service Providers include: (a) cloud infrastructure and hosting providers; (b) payment processors, including Stripe; (c) email delivery and SMS providers, including Twilio and our internal email orchestration service; (d) identity verification and anti-fraud providers; (e) analytics and telemetry providers; (f) customer support platforms, including the JIL Support Intelligence (JSI) system; and (g) professional service providers, including attorneys, accountants, and auditors.

5.3. Disclosures to Affiliates

We may disclose Personal Information to our corporate affiliates for purposes consistent with this Notice. JIL Sovereign Technologies, Inc. is the parent operating company; JIL Sovereign Holdings LLC (Wyoming) is the intellectual property holding entity.

5.4. Disclosures for Legal and Safety Reasons

We may disclose Personal Information in response to a lawful request from a government authority, including a subpoena, court order, warrant, or administrative demand; to comply with an applicable law, regulation, or legal process; to enforce our Terms of Service and Permissible Use Policy; to protect the rights, property, or safety of JIL, our customers, or the public; to prevent or investigate fraud or abuse; or in connection with a suspected or actual violation of the Permissible Use Policy, including reporting to law enforcement, regulatory, or judicial authorities. Where legally permissible, we will provide reasonable notice to the affected user before disclosure.

5.5. Disclosures in Corporate Transactions

In connection with a proposed or consummated merger, acquisition, reorganization, financing, change of control, or sale of all or substantially all of our assets, we may disclose Personal Information to the counterparty, its advisors, and successor entity, subject to customary confidentiality protections.

5.6. Disclosures with Your Consent or at Your Direction

We disclose Personal Information to third parties with your consent or at your direction, for example when you submit a court-admissible evidence bundle to a tribunal or authorize a beneficiary designation under the Secure Document Vault inheritance feature.

5.7. Aggregated and Deidentified Information

We may disclose aggregated and deidentified information that does not identify any individual for research, benchmarking, analytics, product development, and marketing purposes without restriction, provided that we maintain and use such information in deidentified form and make no attempt to reidentify the information.

ARTICLE VI
DATA RETENTION

6.1. Retention Principles

We retain Personal Information for the period necessary to fulfill the purposes described in this Notice, to comply with our legal, accounting, or reporting obligations, to resolve disputes, to enforce our agreements, and to preserve evidentiary integrity with respect to the Services.

6.2. Specific Retention Periods

CATEGORY OF INFORMATION	RETENTION PERIOD
Account profile and authentication data	For the duration of the account plus 7 years following closure, to support audit, dispute, and regulatory requirements.
Transaction and billing records	Minimum 7 years from transaction date, consistent with tax and accounting recordkeeping requirements.
Check request metadata and results	90 days for Quick Checks; 2 years for Deep Checks; 15 years for Evidence Checks and associated CREBs, consistent with evidentiary preservation commitments.
Court-Ready Evidence Bundles (CREBs)	Minimum 15 years from issuance, to support evidentiary re-issuance and authentication under

	Federal Rule of Evidence 902(14).
Secure Document Vault contents	For the duration of the applicable subscription plus a post-termination grace period; longer for documents subject to inheritance designation or CourtChain anchoring commitments.
Monitoring alerts and wallet history	For the duration of the monitoring subscription plus 90 days, except where a CREB has been generated from the alert data.
Customer support correspondence	5 years from last correspondence.
Marketing contact records	Until unsubscribe, plus suppression-list retention indefinite to honor opt-out.
Audit logs and security events	Minimum 7 years.
Dispute submissions (Permissible Use Policy)	5 years from resolution.
Protected persons registry entries	Until removal by registry operator or expiration of underlying protective basis.

6.3. Deletion Upon Account Closure

Upon closure of your account, whether initiated by you or by JIL, we will delete or anonymize your Personal Information except where retention is required under Section 6.2 or otherwise by law. Certain systems may retain Personal Information in encrypted backup media until such backups are rotated out of service, which typically occurs within ninety (90) days.

ARTICLE VII
SECURITY OF PERSONAL INFORMATION

7.1. Security Program

We maintain an information security program designed to protect Personal Information against unauthorized access, disclosure, alteration, and destruction. Our program includes, among other controls: (a) encryption of Personal Information at rest using AES-256-GCM and in transit using TLS 1.3; (b) field-level encryption of Sensitive Personal Information using keys managed by a hardware security module or equivalent; (c) role-based access control, least-privilege principles, and multi-factor authentication for administrative systems; (d) audit logging of access to Personal Information; (e) periodic security testing, including vulnerability scanning and penetration testing; (f) personnel training on security and privacy

responsibilities; (g) vendor management procedures requiring Service Providers to maintain reasonable security; and (h) incident response procedures.

7.2. No Guarantee

No electronic transmission or storage system is impenetrable. We cannot guarantee absolute security. You are responsible for the security of your own credentials, devices, and endpoints.

7.3. Breach Notification

In the event of a security breach that results in the unauthorized acquisition of Personal Information, we will notify affected individuals and applicable regulators in accordance with applicable law.

ARTICLE VIII
YOUR PRIVACY RIGHTS

8.1. Rights Available to All Users

Regardless of your jurisdiction, we offer the following rights to all users of the Services:

(a) the right to access a copy of the Personal Information we hold about you;

(b) the right to request correction of inaccurate Personal Information;

(c) the right to request deletion of your Personal Information, subject to legal retention obligations;

(d) the right to unsubscribe from marketing communications;

(e) the right to close your account.

8.2. California Residents (CCPA / CPRA)

California residents have the rights enumerated above, plus the following under the California Consumer Privacy Act as amended by the California Privacy Rights Act:

(a) the right to know what categories and specific pieces of Personal Information we have collected, the categories of sources, the purposes of collection, and the categories of Third Parties to whom we have disclosed Personal Information;

(b) the right to correct inaccurate Personal Information;

(c) the right to delete Personal Information, subject to exceptions;

(d) the right to opt out of the sale or sharing of Personal Information (which we do not engage in);

(e) the right to limit the use and disclosure of Sensitive Personal Information;

(f) the right to non-discrimination for exercising your privacy rights;

(g) the right to designate an authorized agent to submit requests on your behalf.

8.3. Texas, Virginia, Colorado, Utah, Connecticut, and Other State Residents

Residents of states with comprehensive privacy statutes, including the Texas Data Privacy and Security Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, the Connecticut Data Privacy Act, and analogous laws in other states, have rights substantially similar to those described in Section 8.2, with state-specific variations including the right to appeal a denied request and the right to opt out of targeted advertising, the sale of Personal Information, and profiling in furtherance of decisions that produce legal or similarly significant effects. You may exercise these rights by following the procedures in Section 8.6.

8.4. European Economic Area, United Kingdom, and Other Foreign Jurisdictions

If you are located in the European Economic Area, the United Kingdom, or another jurisdiction whose laws grant additional privacy rights, you may have the right to: (a) access your Personal Information; (b) rectify inaccurate Personal Information; (c) erase your Personal Information under certain conditions; (d) restrict processing under certain conditions; (e) port your Personal Information in a machine-readable format; (f) object to processing based on legitimate interests; (g) withdraw consent where processing is based on consent; and (h) lodge a complaint with a supervisory authority. Our legal bases for processing may include contract performance, legitimate interests, legal obligations, and consent.

8.5. Children

The Services are not directed to children under the age of eighteen (18) and we do not knowingly collect Personal Information from children under 18. If we learn that we have collected Personal Information from a child under 18, we will delete it promptly. Parents or guardians who believe a child has provided Personal Information to us may contact us using the information in Section 9.

8.6. How to Exercise Your Rights

You may exercise your privacy rights by: (a) using the self-service tools available in your account dashboard at retail.jilsovereign.com/dashboard; (b) emailing privacy@jilsovereign.com with your request and sufficient information for us to verify your identity; or (c) writing to the postal address in Section 9. We will respond to verifiable requests within the timeframes required by applicable law, typically within forty-five (45) days. We may require additional information to verify your identity before fulfilling your request. If we deny your request in whole or in part, you

have the right to appeal our decision by responding to our decision email within sixty (60) days; we will respond to appeals within forty-five (45) days.

ARTICLE IX
INTERNATIONAL DATA TRANSFERS

JIL is headquartered in the United States and processes Personal Information in the United States and in other jurisdictions where our Service Providers operate. If you are located outside the United States, please note that U.S. law may provide different protections for Personal Information than the law of your jurisdiction. By using the Services, you acknowledge that your Personal Information may be transferred to and processed in the United States. Where required by law, we implement appropriate safeguards for cross-border transfers, including standard contractual clauses.

ARTICLE X
COOKIES AND TRACKING TECHNOLOGIES

10.1. Types of Cookies We Use

We use cookies and similar tracking technologies for the following purposes:

(a) strictly necessary cookies, which enable essential functionality such as authentication, session management, and security;

(b) performance and analytics cookies, which help us understand how visitors interact with the Services;

(c) functional cookies, which remember your preferences and settings;

(d) security cookies, which help us detect and prevent fraud and abuse.

We do not use cookies for third-party advertising or cross-context behavioral advertising.

10.2. Managing Cookies

You may manage cookies through your browser settings. Disabling cookies may affect the functionality of the Services. We honor Global Privacy Control signals where we are required to do so by law.

ARTICLE XI
NO ADVERTISING; NO SALE OF INFORMATION

JIL does not display third-party advertising in the Services. JIL does not allow advertisers to pay to influence, promote, or alter the content of any Check, Intelligence Output, or other Service output. JIL does not sell Personal Information.

JIL does not share Personal Information for cross-context behavioral advertising. These commitments apply regardless of any changes in applicable law that would otherwise permit such practices, unless and until we provide prior notice to you and update this Notice accordingly.

ARTICLE XII
CHANGES TO THIS NOTICE

We may update this Notice from time to time. When we make material changes, we will update the Effective Date at the top of this Notice and, where required by law or where we determine that changes materially affect your rights, provide additional notice through the Services or by email. Your continued use of the Services after the Effective Date constitutes your acceptance of the updated Notice.

ARTICLE XIII
CONTACT INFORMATION

If you have questions, concerns, or requests regarding this Notice or our privacy practices, please contact us:

JIL Sovereign Technologies, Inc.
Attention: Privacy Officer
[Mailing Address]
Email: privacy@jilsovereign.com
Data Subject Requests: privacy@jilsovereign.com
General: support@jilsovereign.com
Legal notices: legal@jilsovereign.com

For individuals located in the European Economic Area or the United Kingdom, we will identify our representative and, where required, our data protection officer in a subsequent supplement to this Notice.

END OF PRIVACY NOTICE