

PRIVACY POLICY

Effective Date: Jan 1, 2026

Last Updated: May 1, 2026

1. Introduction

FraudScorer Audit Tool ("FraudScorer," "we," "us," or "our") is a Software-as-a-Service (SaaS) platform purpose-built for fraud detection, risk scoring, and audit management. We serve businesses and financial institutions that require robust, data-driven solutions to identify, investigate, and mitigate fraudulent activity across their operations. Our platform delivers real-time risk intelligence, audit workflow management, and compliance-grade reporting in a secure, enterprise-ready environment.

We are deeply committed to protecting the privacy and security of all personal data that passes through our platform, whether belonging to our registered users, enterprise clients, their end customers, or visitors to our website and API endpoints. We handle personal data with the diligence and respect it deserves, and we are committed to transparency about what we collect, how we use it, and the choices available to you.

This Privacy Policy applies to all individuals and entities who interact with FraudScorer, including:

- Visitors to our website and marketing pages;

- Registered users with FraudScorer accounts;
- Enterprise clients and their authorized personnel; and
- Developers and organizations consuming our API services.

By accessing or using the FraudScorer platform, website, or related services, you acknowledge that you have read and understood this Privacy Policy and agree to be bound by its terms. If you do not agree with any aspect of this policy, you should discontinue use of the platform immediately.

2. Information We Collect

FraudScorer collects personal information in several ways depending on how you interact with our platform and services. The categories of information we collect are described in detail below.

2.1 Information You Provide Directly

When you register for a FraudScorer account, engage with our support services, or configure your use of the platform, you may provide the following categories of information directly to us:

- **Account Registration Data:** Full name, business email address, company name, job title, and phone number, collected at the point of account creation or profile update;
- **Billing and Payment Information:** Credit card details, billing address, and invoicing preferences. Note that payment card data is processed exclusively by certified third-party payment processors and is not stored on FraudScorer servers;

- **Support Requests and Communications:** The content of any support tickets, live chat conversations, email correspondence, or feedback submissions you direct to our team; and
- **Configuration Settings and Preferences:** Platform preferences, alert thresholds, workflow configurations, notification settings, and integration parameters you establish within your account.

2.2 Data Processed on Your Behalf (Client Data)

Enterprise clients submit data to FraudScorer for the purpose of fraud scoring, risk analysis, and audit processing. This Client Data may include:

- Transaction records, financial instrument data, account activity logs, and audit trails submitted by clients for real-time or batch fraud scoring;
- User-uploaded documents, records, and datasets provided for audit processing workflows; and
- Any personal data relating to the clients' own customers or end users that is embedded within submitted data sets.

With respect to Client Data, FraudScorer acts solely as a **data processor** operating under the documented instructions of the client, who is the **data controller**. FraudScorer does not independently determine the purposes or means of processing Client Data. Enterprise clients are responsible for ensuring they have a lawful basis to submit personal data to FraudScorer and that their own privacy disclosures to data subjects are accurate and complete.

2.3 Automatically Collected Information

When you access or use the FraudScorer platform, certain information is collected automatically through standard technical mechanisms, including:

- **Log Data:** Internet Protocol (IP) addresses, browser type and version, operating system, pages and features accessed, access timestamps, and referring URLs;
- **Usage Analytics:** Feature interaction patterns, session duration, click-path analysis, and workflow engagement metrics used to understand and improve platform performance;
- **Device Identifiers and Cookies:** Device type identifiers, unique device tokens, and persistent or session-based cookies that support authentication, session continuity, and optional analytics functions; and
- **API Request Metadata:** API endpoint calls, request timestamps, payload sizes, response codes, and authentication token identifiers, retained for security auditing and rate-limit enforcement.

2.4 Information from Third Parties

In certain circumstances, FraudScorer receives personal data from third-party sources to supplement or verify information already held or to enrich fraud detection signals. These sources include:

- **Identity Verification Providers:** Services that corroborate the identity of account holders or platform users during onboarding or high-risk action verification;
- **Credit Reporting and Financial Data Aggregators:** Organizations that supply fraud signal enrichment data, such as bureau indicators, velocity data, or synthetic

identity markers, used to improve risk scoring accuracy;
and

- **Single Sign-On (SSO) Providers:** Identity platforms including Google Workspace, Microsoft Azure Active Directory, and Okta, which may transmit basic profile data (name, email address, organization) to FraudScorer upon user authentication via SSO protocols.

3. How We Use Your Information

FraudScorer uses the personal data we collect for the following lawful purposes:

- **Platform Provision and Operation:** To deliver, operate, maintain, and improve the FraudScorer SaaS platform, including all fraud detection, risk scoring, and audit management features;
- **Client-Directed Processing:** To perform fraud scoring, risk analysis, investigation workflows, and audit functions strictly as directed by enterprise clients under the terms of their service agreements;
- **User Communications:** To send transactional messages, account notifications, security alerts, product updates, and responses to support inquiries;
- **Billing and Subscription Management:** To process payments, issue invoices, manage subscription lifecycles, and handle billing disputes or adjustments;
- **Security and Platform Integrity:** To conduct continuous security monitoring, threat detection, abuse prevention,

vulnerability assessment, and incident response across our systems and infrastructure;

- **Legal and Regulatory Compliance:** To fulfil obligations imposed by applicable law, including anti-money laundering (AML), know-your-customer (KYC), financial regulation, and data protection requirements in jurisdictions where we operate; and
- **Anonymized Analytics and Performance Insights:** To generate aggregated, de-identified statistical analyses of platform performance, feature adoption, and service reliability – used solely for internal improvement purposes.

Important Notice

FraudScorer does **not** use Client-submitted fraud data or audit records for its own independent commercial purposes. We do **not** incorporate Client Data into shared or cross-client artificial intelligence training models without the express, documented, and informed consent of the relevant client.

4. Applicable Privacy Laws

FraudScorer processes personal data in compliance with applicable federal, state, and territorial privacy laws governing users and clients in the United States, Puerto Rico, and U.S. territories. The primary legal frameworks that govern our data practices are described below.

4.1 U.S. Federal Law

At the federal level, FraudScorer's data practices are governed by the Federal Trade Commission Act (Section 5), which prohibits unfair or deceptive practices relating to privacy and data security. Where we process financial data on behalf of enterprise clients, the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations – including the Safeguards Rule – impose additional obligations relating to the protection of nonpublic personal financial information. Sector-specific laws, including applicable provisions of the Bank Secrecy Act (BSA) and anti-money laundering (AML) frameworks, may also apply to certain data processing activities.

4.2 U.S. State Laws

California residents are protected by the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), which grants specific rights regarding personal information (see Section 9.1). FraudScorer also monitors and complies with comparable privacy laws enacted by other U.S. states, including the Virginia Consumer Data Protection Act (CDPA), the Colorado Privacy Act (CPA), and the Texas Data Privacy and Security Act (TDPSA), among others. Users in those states may exercise applicable rights as described in Section 9.2.

4.3 Puerto Rico and U.S. Territories

Residents and users in Puerto Rico, Guam, the U.S. Virgin Islands, American Samoa, and the Northern Mariana Islands are covered by applicable U.S. federal law and relevant territorial statutes. FraudScorer treats such users consistent with our U.S. privacy commitments in their entirety.

5. Data Sharing and Disclosure

FraudScorer does not share personal data except in the circumstances described in this section. We impose contractual obligations on all third parties who receive personal data from us to ensure appropriate safeguards are in place.

5.1 Service Providers and Subprocessors

We engage trusted third-party vendors who process personal data on our behalf as subprocessors, strictly for the purposes of delivering and supporting our services. These categories include:

- **Cloud Infrastructure Providers:** Hosting, storage, content delivery, and database services that underpin platform operations;
- **Payment Processors:** PCI-DSS compliant processors that handle payment card and billing transactions on our behalf;
- **Analytics Providers:** Tools used to gather aggregated, anonymized platform usage data for performance monitoring;
- **Email and Communication Services:** Providers that facilitate transactional emails, security alerts, and support ticket routing;
- **Security and Monitoring Tools:** Intrusion detection, log management, and vulnerability scanning services that protect platform integrity.

A current list of our authorized subprocessors is maintained and made available to enterprise clients upon written request. FraudScorer will notify enterprise clients of material changes to the subprocessor list in accordance with applicable Data Processing Agreements.

5.2 Business Transfers

In the event of a merger, acquisition, reorganization, or sale of all or substantially all of our assets, personal data held by FraudScorer may be transferred to the successor entity. We will provide notice of any such transfer via email or prominent in-platform notification, and the successor entity will be required to honor the commitments made in this Privacy Policy or provide comparable protections.

5.3 Legal Requirements

FraudScorer may disclose personal data where required or permitted by law, including in response to:

- Valid subpoenas, court orders, or enforceable governmental or regulatory directives;
- Requests from law enforcement agencies acting within their lawful authority; and
- Circumstances where disclosure is necessary to protect the rights, property, or physical safety of FraudScorer, its users, clients, or the general public.

Where legally permissible, FraudScorer will notify affected clients or users of any compelled disclosure request prior to complying.

5.4 With Your Consent

Beyond the circumstances described in this section, FraudScorer will not share your personal data with third parties without obtaining your prior, explicit, and informed consent. You retain the right to withdraw any such consent at any time.

5.5 We Do Not Sell Personal Data

No Sale of Personal Data

FraudScorer does **not** sell, rent, lease, or otherwise trade personal information to any third party for their own marketing, commercial, or advertising purposes. This prohibition applies to all data, including information subject to the California Consumer Privacy Act (CCPA) and its amendments under the California Privacy Rights Act (CPRA).

6. Data Retention

FraudScorer retains personal data only for as long as is necessary to fulfil the purposes for which it was collected, to comply with legal and regulatory obligations, and to resolve disputes or enforce our agreements. The following retention schedules apply:

- **Account Data:** Retained for the duration of the active contractual relationship, plus a period of seven (7) years following termination to satisfy applicable legal, compliance, and audit obligations;
- **Client-Submitted Audit and Fraud Data:** Retained strictly in accordance with the terms agreed upon in the applicable enterprise service agreement. Upon contract termination, such data will be securely deleted or returned to the client as specified in the agreement;
- **Log and Usage Data:** Automatically purged after twelve (12) months from the date of collection, except where retention is required for ongoing security investigations or legal proceedings;

- **Backup Data:** Residual copies of deleted data present in encrypted backup systems will be overwritten within ninety (90) days of the deletion request being processed.

You may request early deletion of your personal data at any time by contacting our Privacy Team (see Section 14). Such requests will be honored subject to our legal obligation to retain certain records under applicable law. Where a legal hold prevents immediate deletion, we will inform you of the applicable retention period.

7. Data Security

FraudScorer maintains a comprehensive, enterprise-grade security program designed to protect personal data against unauthorized access, alteration, disclosure, or destruction. Our security measures include, but are not limited to, the following:

- **Encryption:** All data in transit is protected using Transport Layer Security (TLS) version 1.2 or 1.3. All data at rest is encrypted using AES-256 encryption across our storage infrastructure;
- **Access Controls:** Role-Based Access Control (RBAC) ensures that personnel and system components can access only the data necessary for their authorized functions. Multi-Factor Authentication (MFA) is enforced for all administrative accounts and is strongly recommended for all user accounts;
- **SOC 2 Type II Compliance:** FraudScorer maintains an active SOC 2 Type II audit program, validating our security, availability, and confidentiality controls against the AICPA Trust Services Criteria on an annual basis. Reports

are available to enterprise clients under non-disclosure agreement;

- **Penetration Testing and Vulnerability Management:** We conduct regular third-party penetration tests and continuous automated vulnerability scanning across our application, infrastructure, and API layers;
- **Incident Response:** We maintain documented incident response procedures with defined roles, escalation paths, and notification timelines. In the event of a confirmed personal data breach, affected clients and individuals will be notified in accordance with applicable legal requirements (including within applicable state and federal notification timelines);
- **Personnel Security:** All FraudScorer employees and contractors with access to personal data undergo pre-employment background screening and receive mandatory data protection and security awareness training upon onboarding and annually thereafter.

Security Disclaimer

While FraudScorer employs commercially reasonable and industry-standard safeguards, no security measure is absolutely infallible. Users are responsible for maintaining the confidentiality of their account credentials and must notify FraudScorer immediately upon suspecting any unauthorized use of their account.

8. Data Storage and Location

FraudScorer's data processing infrastructure is located entirely within the United States. All personal data collected through the platform – including account data, Client Data, and usage logs – is stored and processed on U.S.-based servers operated by our cloud infrastructure providers. FraudScorer does not transfer personal data outside of the United States in the ordinary course of its operations.

- **U.S.-Based Data Centers:** All primary and backup data storage occurs within U.S.-based cloud infrastructure facilities, subject to U.S. federal and state data protection requirements; and
- **No Cross-Border Transfers:** FraudScorer does not route, store, or otherwise transfer personal data to data centers or third parties located outside the United States.

Enterprise clients may request a copy of the applicable Data Processing Agreement (DPA) by contacting our Privacy Team at privacy@fraudscorer.com.

9. Your Privacy Rights

Depending on your jurisdiction of residence, you may have specific legal rights regarding the personal data that FraudScorer holds about you. We are committed to facilitating the exercise of these rights promptly and without undue friction.

9.1 Rights for California Residents (CCPA / CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

- **Right to Know:** To request disclosure of the categories and specific pieces of personal information we have collected, the sources of that information, our business or commercial purposes for collecting it, and the categories of third parties with whom we share it;
- **Right to Delete:** To request deletion of your personal information, subject to certain exceptions permitted by law;
- **Right to Correct:** To request correction of inaccurate personal information we maintain about you;
- **Right to Opt Out of Sale or Sharing:** To opt out of the sale or sharing of your personal information. As stated in Section 5.5, FraudScorer does not sell or share personal information for cross-context behavioral advertising; and
- **Right to Non-Discrimination:** FraudScorer will not discriminate against you for exercising any of your CCPA/CPRA rights, including by denying services, charging different prices, or providing a different level or quality of service.

Categories of personal information collected include: identifiers (name, email, IP address), professional or employment-related information, commercial information (billing records), internet or other electronic network activity information, and inferences drawn to create a profile about you. California residents may also contact the California Privacy Protection Agency (CPPA) if they believe their rights have not been honored.

9.2 Rights for Other U.S. State Residents

Residents of other U.S. states – including Virginia, Colorado, Texas, Connecticut, Utah, and others with enacted comprehensive

privacy laws – have similar rights regarding their personal data, which may include the right to access, correct, delete, and opt out of certain processing activities. FraudScorer extends these rights to all U.S. residents regardless of state and will process requests in accordance with the law applicable to the requestor's state of residence. Users may submit requests using the contact information in Section 9.3.

9.3 How to Exercise Your Rights

To submit a privacy rights request or inquiry, you may use any of the following channels:

- **Contact us:** ww.fraudscorer.com
- **Response Timeline:** FraudScorer will acknowledge receipt of your request within five (5) business days and will respond substantively within thirty (30) calendar days. Where legally permitted, this period may be extended by up to an additional forty-five (45) days, with notice provided to you explaining the reason for the extension.
- **Identity Verification:** To protect your personal data, we may require verification of your identity before processing certain requests. You will be informed of any verification requirements at the time of your request.

10. Cookies and Tracking Technologies

FraudScorer uses cookies and similar tracking technologies to enable essential functionality, analyze platform usage, and – where you have provided consent – to support marketing and personalization activities. The categories of cookies we use are as follows:

- **Strictly Necessary Cookies:** Required for the platform to function. These include session authentication tokens, CSRF protection cookies, and load-balancing identifiers. These cookies cannot be disabled without impairing core functionality;
- **Functional Cookies:** Retain your preferences and settings (such as language, display options, and notification configurations) to deliver a personalized experience across sessions;
- **Analytics Cookies:** Collect anonymized data on how users interact with the platform, including pages visited, features used, and session duration, used solely to improve the platform. Activated only upon consent; and
- **Marketing Cookies:** Used to deliver relevant promotional content and measure the effectiveness of marketing campaigns. Activated only upon explicit consent.

On your first visit to FraudScorer, a cookie consent banner will be presented allowing you to accept or decline non-essential cookie categories. You may update your cookie preferences at any time through your account settings or browser controls. Most browsers allow you to block, delete, or receive alerts about cookies through their settings menus.

FraudScorer respects Do Not Track (DNT) signals where technically feasible. Where a valid DNT signal is detected, non-essential analytics and tracking functions will be suppressed for that session.

11. Children's Privacy

The FraudScorer Audit Tool is designed and intended exclusively for business-to-business use by professionals and enterprise clients within regulated industries. The platform is not directed at, nor intended for use by, individuals under the age of eighteen (18) years.

FraudScorer does not knowingly collect, solicit, or process personal data from minors. If we become aware that personal data has been submitted by or relating to an individual under the age of 18 without verifiable parental or guardian consent, we will take prompt steps to delete such data from our systems. If you believe that we may have inadvertently collected such data, please contact us immediately at privacy@fraudscorer.com.

12. Third-Party Links and Integrations

The FraudScorer platform may contain hyperlinks to third-party websites or may offer integration capabilities with external services, applications, or data providers. These third-party services operate under their own independent privacy policies and data protection practices.

FraudScorer is not responsible for, and does not endorse or control, the privacy practices, security standards, or content of any third-party website or service. Users and clients are strongly encouraged to review the privacy policies of any third-party service they access through or alongside the FraudScorer platform before providing personal data to that third party.

The presence of a link or integration capability within the FraudScorer platform does not constitute an endorsement of the third party's data handling practices by FraudScorer.

13. Changes to This Privacy Policy

FraudScorer reserves the right to modify, update, or replace this Privacy Policy at any time to reflect changes in our practices, technology, legal requirements, or for other legitimate operational reasons. All updates will be reflected by a revised "Last Updated" date at the top of this document.

For material changes – those that significantly alter the nature of the data we collect, our purposes for using it, or your rights – FraudScorer will provide advance notice of at least thirty (30) days prior to the effective date of the change. Such notice will be delivered via:

- A direct email notification to the primary contact address associated with your account; and/or
- A prominent in-platform notification displayed upon login.

Your continued use of the FraudScorer platform following the effective date of any updated Privacy Policy constitutes your acceptance of the revised terms. If you do not agree with the changes, you must cease using the platform and may request account closure and data deletion as described in Section 9.3 of this Policy.

Prior versions of this Privacy Policy are archived and available upon written request to our Privacy Team.

14. Contact Information

If you have questions, concerns, or requests relating to this Privacy Policy or the way FraudScorer handles your personal data, please contact us using the details set out below.

Contact Role	Details
Company	Acquisition & Reason L.L.C.
Privacy Inquiries	www.fraudscorer.com ATT: Privacy Inquires
Mailing Address	5900 Balcones Dr. Suite 100 Austin TX 78731
California Residents	You may also contact the California Privacy Protection Agency (CPPA) at cppa.ca.gov

We endeavour to respond to all legitimate privacy inquiries within five (5) business days of receipt. For formal rights requests, please refer to the timelines set out in Section 9.3.