Sift Logo Several
blue dots forming

Sift Service Privacy Notice

Effective: January 1, 2020

Previous Service Privacy Notice available here

OUR COMMITMENT TO PRIVACY

Sift Science, Inc. (**"Sift"**, **"we"** or **"us"**) respects your privacy and wants you to be informed about what we do. Sift provides a suite of digital trust and safety products (the **"Sift Services"**) designed to help online businesses (our **"Customers"**) detect and prevent fraud and other malicious behavior on their digital properties, such as their websites and mobile applications (**"Customer Sites"**).

This Service Privacy Notice (this **"Notice"**) explains who we are and how we collect, share, and use personal information about you when: (i) you use the Sift Services as an authorized end user under our Customer's (your employer's) account (**"Authorized User"**); or (ii) you interact with any of the Customer Sites that use the Sift Services as a digital end user (**"End User"**). We also include information about how you can exercise your privacy rights. **"You"** or **"your"** may be an End User and/or Authorized User depending on the context.

Please note that this Notice does not describe our collection and use of personal information when visitors access our website. For information about how we collect and use information via our website (www.sift.com and its subdomains), please see our Website Privacy Notice.

Quick links

We recommend that you read this Notice in full to ensure that you are fully informed. However, if you would like to access a particular section of this Notice, then you can click on the relevant link below to jump to that section.

PART I. GENERAL INFORMATION AND KEY TERMS

Who we are

Sift is a Software-as-a-Service (SaaS) company based in San Francisco, California. We help our Customers detect and address fraud and other malicious behavior on their Customer Sites using our proprietary real-time machine learning technology.

In doing so, we need to collect and process information about End Users who interact with Customer Sites. Our cloud-based machine learning platform uses this information to predict and prevent fraudulent activity in real time.

We have three core product offerings for our Customers: Payment Protection (reduces fraudulent payments), Account Defense (reduces fake account creation and prevents bad actors from accessing trust-worthy accounts) and Content Integrity (protects Customer Sites from malicious content). You can find out more about these offerings here.

How the Sift Services work

Customers provide us with data and information about End Users and their interactions with the applicable Customer Sites through our Application Programming Interfaces (APIs). In addition, we collect data directly from End Users through standard tracking technologies (like our JavaScript code or SDK), which our Customers can embed on their Customer Sites. We refer to all of this data as **"Customer Data"** - as described in Part II below.

We then process the Customer Data through our cloud-based machine learning platform to return a relative fraud score which is a numerical indicator of the likelihood of fraud for a particular event on the Customer Site (e.g., a purchase transaction, the posting of content, creation of a profile). In addition to the score, we provide our Customers with supporting evidence for the score and aggregated reporting and insights.

The fraud score, supporting evidence, and insights are used by Customers to assist them in identifying and preventing fraudulent activity on their Customer Sites. It is up to our Customers to decide what action to take or not to take using the information we provide. For example, depending on the rules set by our Customers, transactions with certain scores may be presented with further authentication challenges, flagged for the Customer's review, or blocked. Typically, however, the transaction or activity will proceed with no issues. More information about what to do if a transaction is blocked is provided in the "Automated Decision-Making" section below. Customers also provide us with ongoing feedback on the accuracy of the scores by reviewing the activity on their Customer Sites, which in turn improves our proprietary modeling and algorithms.

PART II. WHAT WE COLLECT AND HOW WE USE IT

(A) END USERS

Information We Collect About End Users

Information provided by our Customers: Our Customers decide the type of Customer Data they wish to send to Sift for analysis within the Sift Services. Our solutions and support teams work closely with Customers to assess the utility of the specific Customer Data they send to us. For example, Sift guides Customers as to whether a particular data type (e.g., billing method) may be relevant in assessing the particular activity (e.g., likelihood of stolen payment credentials). While it will depend on the specific product offering and Customer relationship, the Customer Data that Customers typically send to us through our API integration include:

- **Contact details** (such as your email address, postal address, phone number, and user login);
- **Information about your device** (such as your IP address, session ID, mobile/desktop device properties, and metadata);
- **Transaction information** (such as information about items you've purchased on Customer Sites, currency codes, billing method, and partial credit card information); and
- **Customer Site communication information** (such as feedback, messaging, reviews or images you may have provided on or within Customer Sites).

Information we automatically collect when you visit Customer Sites: As further explained below, we use certain standard tracking technologies to automatically collect certain information about your device when you interact with and use Customer Sites. Some of this information (including, for example, your IP address and certain unique identifiers), may identify a particular computer or device and may be "personal data" in some jurisdictions, including the EU. Depending on whether you visit a Customer Site via an app or a webpage, the information we collect includes:

- **Browser and device information,** such as the device type and model, manufacturer, operating system type and version (e.g. iOS or Android), web browser type and version (e.g., Chrome or Safari), user-agent, carrier name/code and country code, time zone, the network connection type, IP address, hardware-based identifiers (e.g. MAC address), host name, device identifiers (such as iOS Identifier for Advertisers (IDFA), Android/Google Advertising ID (AAID or GAID)), canvas fingerprint, characteristics related to emulation or rooted (such as if your device is "jailbroken"), and app name and version. We also collect character set, host name, language, page title and URL, referrer URL, number of fonts, fonts hash, number of plugins, plugins hash, screen height and width, color depth, platform, cookie footprint, maximum touch points, JavaEnabled, session storage, local storage, whether the resolution has been tampered, language or OS, whether ad blocking is enabled, whether do not track is enabled, flash socket IP and flash identifier. The SDK will also collect phone-related metadata (battery level, device properties, carrier name); and
- **Information about an End User's behavior on Customer's Sites,** such as information about the activities on those Customer Sites, session ID, session start/stop time, timezone offset, and location information which may be general location information inferred from your IP address or, in some circumstances, more precise geolocation information based on latitude and longitude coordinates. You may be able to control the collection of location information through particular Customer Sites by changing the preferences on your mobile device.

Information we collect from third party sources: We combine or enhance the information we collect about you with limited information we receive from third parties. For example, we receive information such as whether an IP address is commercial or private, whether a phone number is a landline, whether an email domain is free, or the issuing bank associated with a transaction. We also work with a small number of providers that match information from social media with End Users' email addresses provided to us, or provide us with a human-readable, mapped location based on a physical address or latitude/longitude.

How We Use End Users Information and the Legal Bases

Sift only uses Customer Data to provide, maintain, improve, and develop the Sift Services.

For example, we process Customer Data through our cloud-based machine learning platform to return fraud scores to our Customers for particular events or activities on the Customer Site. We may also use Customer Data to optimize and improve the Sift Services (for example, to train our proprietary models and algorithms so that we can more effectively detect fraudulent behaviors).

We base our processing of your personal information on: (i) our legitimate interests in operating the Sift Services and better detecting and preventing fraud and malicious behavior on Customer Sites;

and (ii) our (and our Customers) legitimate interest in combating fraud and maintaining safe online experiences for our Customers and their End Users.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, including any legitimate interests relied upon, please contact us as provided under the How to contact us section at the end of this Notice.

How We Use Tracking Technologies to Collect Information about End Users

We use standard tracking technologies to automatically collect certain information (as described in the Information We Collect About End Users section) from your device and/or browser when you visit or interact with Customer Sites.

We use the following tracking technologies:

- **JS Snippet:** A JavaScript code (**"JS Snippet"**), also called a tag or pixel, is a tiny snippet of code inserted into the content of the Customer Site.
- **Mobile "SDKs" or "Software Development Kits":** These are blocks of code that are embedded into a Customer Site that allow Sift to collect certain information as further described above.
- **Canvas Fingerprinting:** We use canvas fingerprinting, which is a tracking technique that allows us to render graphic images from built-in features of HTML5 Canvas in your browser. The canvas image is often rendered differently on different devices because of a number of factors (such as, your web browser version, operating system and its settings, and installed graphics hardware), and this will allow us to distinguish you from other End Users.

Automated Decision-Making

Automated decision-making means that a decision is made automatically on the basis of a computer determination (using software algorithms), without human review or intervention. The services we provide to our Customers may result in an automated decision being made by our Customers about an action you have made on a Customer Site. For example, in certain limited circumstances, the Customer may use the analysis we provide them to automatically pause the completion of an activity or transaction based on rules the Customer has set. In such instances, you may be required to take further steps (e.g., two factor authentication) or you may potentially be unable to complete a transaction. Please contact the relevant Customer directly for more information.

(B) AUTHORIZED USERS

Information We Collect About Authorized Users

Information you provide to us when you use the Sift Services: You (or your organization's administrator) may provide certain personal information to us through the Sift Services – for example, when you register for the Sift Services, when you consult with our customer support, send us an email or communicate with us in any way in connection with the Sift Services.

The personal information we collect may include:

- **Business contact information**(such as your name, job title, organization, address, and email address);
- **Account log-in credentials** (such as your username and password);
- **Troubleshooting and support data** (which is data you provide when you contact Sift for help, such as the products you use, and other details that help us provide support); and
- **Payment information** (if you pay for the Sift Services, our payment processor will collect certain information required to process your payment, such as your credit card number and associated identifiers, billing address and background information. Sift does not store full credit card data).

If you ever communicate directly with us, we will maintain a record of those communications and responses.

Information we collect automatically when you use the Sift Services: In connection with your organization's deployment of the Sift Services, we may automatically collect certain device and usage data about Authorized Users when they interact with and use the Sift Services (we call this information "Usage Data"). We (or our third party service providers) use cookies, web beacons, and other tracking technologies to collect some of this information. Please review the Sift Website Cookie Notice for further information.

Usage Data may include:

- **Usage data** (such as the dates and times you access the Sift Services, page views, which activities and features you use, the links you click on, and how you interact with the Sift Services);
- **Device data** (such as IP address, device type, operating system and Internet browser type, screen resolution, operating system name and version, device manufacturer, and model);
- **Device event information** (such as system activity, error reports (sometimes called 'crash dumps'), and hardware settings); and
- **Log files** automatically generated during the use of the Sift Services (such as access times, hardware, and software information).

How We Use Authorized Users Information and the Legal Bases

We collect and process personal information for the purposes and on the legal bases identified below. For these purposes, we combine data we collect from different contexts (for example, from your use of two products within the Sift Services). We use this information to:

- **Provide the Sift Services:** We base our processing of your personal information on our legitimate interests to operate and administer the Sift Services. For example, to process transactions with you, authenticate you when you log in, provide customer support, and operate and maintain the Sift Services;
- **Promote the security of the Sift Services:** We process your personal information by tracking use of the Sift Services, creating aggregated, non-personal information, verifying accounts and

activity, monitoring suspicious or fraudulent activity, and enforcing our terms and policies, to the extent this is necessary for our legitimate interest in promoting the safety and security of the Sift Services, systems, and applications and in protecting our rights and the rights of others;

- **To improve and develop the Sift Services:** We use your personal information (including Usage Data as described in the Information We Collect About Authorized Users section) to identify trends, usage, activity patterns, and areas for integration and improvement of the Sift Services so that we continually improve the Sift Services, including adding new features or capabilities that make the Sift Services smarter, faster, secure, integrated, and more useful to our Customers and their Authorized Users to the extent it is necessary for our legitimate interests in developing and improving the Sift Services, or where we seek your consent;
- **To communicate with you about the Sift Services:** We may send you service, technical, and other administrative or transactional emails, messages, and other types of notifications to in reliance on our legitimate interests in administering the Sift Services. These communications are considered part of the Sift Services and in most cases you cannot opt-out of them. If an opt-out is available, you will find that option within the communication itself or in your account settings;
- **Send you marketing communications:** We will process your personal information to send you marketing information, product recommendations, events, promotions, contests, and other non-transactional communications (e.g., emails, telemarketing calls, SMS or push notifications) about us in accordance with your marketing preferences as necessary for our legitimate interests in conducting direct marketing or to the extent you have provided your prior consent (please see the Unsubscribe from our mailing list section below);
- **To protect our legitimate business interests and legal rights:** Where required by law or where we believe it is necessary to protect our legal rights, interests, and the interests of others, we use information about you in connection with legal claims, compliance, regulatory, and audit functions, and disclosures in connection with the acquisition, merger, or sale of a business; and
- **With your consent:** We use information about you where you have given us consent to do so for a specific purpose not listed above. For example, we may publish testimonials or featured customer stories to promote the Sift Services with your permission.

(C) SHARING INFORMATION WITH THIRD PARTIES

We may share and disclose information about End Users and Authorized Users in the following circumstances:

- **Vendors, consultants and other service providers**
  We may share your information with third party vendors, consultants, and other service providers who provide data processing services to us and with whom the sharing of such information is necessary to undertake that work. If you are an Authorized User, examples of the type of service providers include: processing billing, providing customer support, or hosting our infrastructure. We may use providers who assist us in delivering online and offline marketing optimizations. If you are an End User, examples of these types of service providers

include: hosting our infrastructure and for data enrichment purposes (described below).

- **Service Providers for Data Enrichment**
  We may share minimal Customer Data (e.g., email addresses) with select third-party service providers (e.g., location data providers or identity verification providers) for data enrichment purposes. Enriching data allows us to make more informed fraud risk assessments. For example, we may work with providers that match information from social media with End Users' email addresses provided to us, that provide us with a human-readable, mapped location based on a physical address or latitude/longitude. Sift requires that any information disclosed to a provider is used only to perform their service and not for any incompatible purpose, and only as allowed by applicable law.
- **Professional advisors**
  We may disclose your personal information to professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services they render to us.
- **Compliance with laws**
  We may disclose your information to any competent law enforcement body, regulator, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person (see below).
- **Vital interests and legal rights**
  We may disclose information about you if we believe it necessary to protect the vital interests or legal rights of Sift, you or any other person.
- **Corporate Affiliates and Transactions**
  We may provide your information to our affiliates (meaning any subsidiary, parent company or company under common control with Sift). Our affiliates will use your information only for the purposes described in this Notice. Additionally, if Sift is involved in a merger, acquisition or sale of all or a portion of its assets, your information may be shared or transferred as part of that transaction, as permitted by law.

PART III. INTERNATIONAL TRANSFERS, SECURITY AND DATA RETENTION

Processing of personal information in the US and other territories

Your personal information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country. Specifically, our servers are located in the United States, and our third party service providers and partners operate around the world. This means that when we collect your personal information we may process it in different countries. However, we have taken appropriate safeguards to require that your personal information will remain protected in accordance with this Notice.

EU-US and Swiss-US Privacy Shield Frameworks

With respect to personal information we receive in the United States concerning individuals in the EU and Switzerland, we comply with the EU-US and Swiss-US Privacy Shield Frameworks as set forth by the US Department of Commerce when we transfer personal information from the European Union, the United Kingdom, and Switzerland to our servers in the United States for processing. Please see our Privacy Shield Notice to learn more. If there is any conflict between the terms in this Notice and the Privacy Shield Principles (as set out in the Privacy Shield Frameworks), the Privacy Shield Principles shall govern.

PART IV. YOUR PRIVACY RIGHTS

Depending on your location and subject to applicable law, you may have the following rights with regard to personal information we control about you:

Access, review, change, update or delete your information (EEA, UK, and Swiss residents)

If you are a resident of the European Economic Area ("EEA"), United Kingdom, and Switzerland, you may access, review, modify, and request deletion of any personal information that we process about you, as required by law. You can send an email to privacy@sift.com to exercise these rights.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. To protect your privacy and security, we may need to take reasonable steps to verify your identity before responding to your request.

Objection to processing of, or requesting restriction or portability of personal information (EEA, UK, and Swiss residents)

In addition, if you are a resident of the European Economic Area EEA, United Kingdom, and Switzerland, and we can properly verify your identity, you can object to the processing of your personal information, ask us to restrict the processing of your personal information or request portability of your personal information. To exercise these rights, email privacy@sift.com.

Withdrawal of consent (EEA, UK, and Swiss residents)

If you are a resident of the EEA, United Kingdom, or Switzerland, and we have collected and process your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. To withdraw your consent to any processing, email privacy@sift.com.

Right to complain to a data protection authority (EEA, UK, and Swiss residents)

If you are an End User located in the EEA, UK or Switzerland, you have the right to complain to a data protection authority about our collection and use of your personal information. For more

information, please contact your local data protection authority. Contact details for data protection authorities in the EEA and UK are available here and Switzerland are here.

California CCPA Rights: for California Residents

When we handle personal information (as defined under the California Consumer Privacy Act, or CCPA) in providing the Sift Services to our Customers, we do so as a provider of services to and/or on behalf of our Customers (who are “businesses” under the CCPA), to assist them in protecting against illegal or fraudulent activity. When requested, we reasonably assist our Customers in responding to consumer requests under the CCPA. Please direct any requests regarding your CCPA rights to the businesses you believe may have collected (or transferred to Sift) your information, so that those businesses can properly instruct us whether and how to assist them in responding. Where we are the party acting as the “business” (for instance, if we have marketed to you) we are the correct party to address these requests. To learn more about how to make a consumer request, please contact us at privacy@sift.com, or view the privacy rights section in our Website Privacy Notice.

Unsubscribe from our mailing list

You may at any time ask us to stop sending marketing communications to you, including by clicking "Unsubscribe" in any e-mail communications we send you. If you have any questions in relation to the "Unsubscribe" process, please feel free to get in touch via the contact details set out below. If you choose to no longer receive marketing information, we may still communicate with you regarding such things as your security updates, product functionality, responses to service requests, or other transactional, non-marketing/administrative related purposes.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. To protect your privacy and security, we may need to take reasonable steps to verify your identity before responding to your request.

PART V. OTHER IMPORTANT INFORMATION

Security safeguards

We use technical and organizational security measures designed to protect personal information processed as part of the Sift Services against unauthorized access, disclosure, alteration, and destruction.

Data retention

We retain your personal information where we have an ongoing legitimate business need to do so and for a period of time consistent with the original purpose as described in this Notice. We determine the appropriate retention period for personal information on the basis of the amount, nature and sensitivity of your personal information processed, the potential risk of harm from unauthorized use or disclosure of your personal information and whether we can achieve the

purposes of the processing through other means, as well as on the basis of applicable legal requirements (such as applicable statutes of limitation). If you are an End User located in the EEA, United Kingdom or Switzerland we retain your personal information for up to four years from the date of collection.

After expiration of the applicable retention periods, we will either delete or anonymize your personal information or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Children and Sensitive Information

We do not knowingly collect personal information from anyone under 13 years of age, and in the EEA, UK, or Switzerland, 16. Similarly, we do not knowingly collect or utilize any sensitive personal information, such as health information, full financial account information, or government identifiers. In the EEA, we do not knowingly collect or utilize any personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying an individual, or data concerning an individual's health, sex life, or sexual orientation. We ask that you not provide us with such information.

Changes to this Notice

We may revise this Notice from time to time in response to changing legal, technical or business developments, and the revised version will be effective when it is posted. If we make any material changes to the ways in which we use or share personal information previously collected from you, we will post the updated version here and notify you and/or the Customer by email, by means of a prominent notice on our website, or by other means. You can see when this Notice was last updated by checking the "last updated" or "effective" date displayed at the top of this Notice.

PART VI. HOW TO CONTACT US

Contact Details

Please contact Sift with any questions or comments about this Notice or our privacy practices at:

Sift Science, Inc.
Attn: Privacy Officer
123 Mission Street, 20th Floor
San Francisco, CA 94105
Email: privacy@sift.com

Controller Status, Data Protection Officer and EU Representative

If you are a resident in the EEA, UK, or Switzerland, Sift Science, Inc. is the controller of the

personal information (i.e., personal data under European data protection legislation) collected through the Sift Services.

You may contact our Data Protection Officer by emailing dpo@sift.com or using the mailing address listed in the Contact Details section above. Our EU representative (for EEA, UK or Swiss data subjects) is:

Sift Science Ireland Limited
by email: privacy@sift.com
by mail: Sift Science Ireland Limited c/o Sift Science, Inc. 123 Mission Street, Suite 2000, San Francisco, CA 94105

Further Privacy Resources

Website Privacy Policy

Privacy Shield Notice

Website Cookie Notice

Terms of Service

Our newsletter delivers industry trends, insights, and more.

Email Address

Subscribe

You can unsubscribe at any time. Please see our Website Privacy Notice.

If you are using a screen reader and are having problems using this website, please email support@sift.com for assistance.

PRIVACY & TERMS