

Sift Service Privacy Notice

Last Updated: May 18, 2018

PART I. GENERAL INFORMATION

Our commitment to privacy

Sift Science, Inc. ("**Sift**") provides digital trust products and services (the "**Sift Service**") to online businesses (our "**Customers**") to help them detect and address fraud and other malicious behavior on their digital properties.

This Sift Service Privacy Notice ("**Notice**") explains how we collect, share and use personal information in the context of the Sift Service. In using our service, Customers provide Sift with information about their users' activities for fraud analysis. That information may include your personal information. This Notice provides an explanation of the Sift Service and how you can exercise your privacy rights with respect to your personal information.

This Notice does not describe our collection and use of personal information when visitors access our website or in connection with our sales and marketing efforts. For that information, please see our [Site Privacy Notice](#).

Introduction to Sift Service

The Sift Service begins when Customers provide us with data and information about their users ("**Users**") and their interactions with the applicable Customer Site ("**Service Data**"). Customers provide that Service Data through multiple technologies including cookies, web beacons, Javascript code and other data collection technologies, our REST Application Programming Interfaces and the Sift Service management console, as further described in Part II below. We take the Service Data and use our proprietary analytics algorithms to convert it into a holistic and relative fraud score concerning the specified activity on the Customer Site (e.g. purchase transactions, public profile creation or postings, etc.). This assists in identifying and preventing fraudulent activity on the applicable Customer Site.

Our Customers then decide what action to take, or not to take, based on the analysis Sift provides to them. For example, they may choose to block a transaction if they believe there is a high risk of it being a fraudulent transaction. Customers also provide us with ongoing

feedback on the accuracy of our service results by reviewing transactions and activity for fraud.

Quick Links

- [PART I. GENERAL INFORMATION](#)
- [PART II. WHAT THE SERVICE COLLECTS AND HOW WE USE IT](#)
- [PART III. CUSTOMER INFORMATION WE COLLECT AND HOW WE USE IT](#)
- [PART IV. SHARING INFORMATION AND SECURITY](#)
- [PART V. YOUR PRIVACY](#)
- [PART VI. ADDITIONAL INFORMATION FOR EEA RESIDENTS](#)
- [PART VII. CHANGES AND HOW TO CONTACT SIFT](#)

PART II. WHAT THE SERVICE COLLECTS AND HOW WE USE IT

Service Data that our Customers provide to us

Our Customers decide the types / format of Service Data they wish to send to Sift for analysis using the Sift Service. We encourage Customers to work closely with the Sift solutions and support teams to assess the utility of the specific Service Data they send to us. Our goal is to help Customers assess whether certain activity is problematic, for example, helping to assess the likelihood that payment information has been stolen or that a User's identity is false.

Specifically, Customers may send Sift personal information provided by Users, such as email addresses, billing addresses, shipping addresses, user login name, and telephone numbers. Customers may send us information about specific User behavior on their Customer Sites, including the IP address of the device used, the pages navigated by the User, time of login/logout, items viewed, added to cart or purchased. Customers may send data points about the form of payment, such as order amount, payment method, partial credit card numbers, and order status.

In addition, Customers may provide us with information about commentary that Users leave on their Customer Sites (e.g. forum posts and product reviews). This information helps Sift catch inappropriate content so that our Customers can operate cleaner services.

Customers may also place JavaScript code issued by Sift ("**Sift JS Snippet**") onto their Customer Sites in order to enable us to collect unique device identifiers, including device metadata, from Users automatically. The Sift JS Snippet collects information to uniquely identify the device the User is using. From time to time, we may alter our device fingerprinting technology to improve its effectiveness at identifying a device.

Similarly, in connection with their mobile applications, Customers may integrate with Sift-provided SDKs to help prevent fraud that may occur through their applications. The SDKs may enable Sift to collect more precise information about the user's location, such as GPS (if the

location settings allow it) and IP address. Additionally, the SDK may collect phone-related metadata (e.g. battery level, device properties, carrier name, motion and proximity information) and unique device identifiers.

Use of Service Data

Sift uses the Service Data for the limited purpose of providing fraud detection and prevention services to Customers of the Sift Service. Sift does not receive or process Service Data for any other purpose. The security of all of the Service Data we receive is protected by Sift as further described below.

PART III. CUSTOMER INFORMATION WE COLLECT AND HOW WE USE IT

Information we collect about our Customer's employees and agents (the "Customer Information") and how we use it

We will collect information about each Customer when they register for the Sift Service, such as company name, URL, fraud-related information, and company size. We also collect personal information of those individuals that represent Customer in connection with the use of the Sift Service, such as full name, email address, phone number. We will use that information for correspondence concerning Customer's use of the Sift Service, for example, to arrange billing and to provide customer support. If the Customer pays by credit card, our payment processor will collect that information (Sift does not store full credit card data).

We may also use the information individuals provide to us for our marketing purposes. Any recipients of marketing information will always be able to opt-out of receiving marketing information at any time (see the "Unsubscribe from Our Mailing List" section below). We will still communicate with applicable Customer team members regarding such things as product functionality, security updates, support or other service related reasons.

We also use Customer Information to analyze Customers' use of the Sift Service for business analytics and to maintain, develop and improve the Sift Service.

PART IV. SHARING INFORMATION AND SECURITY

Sharing and disclosure of information to third parties

Vendors, consultants and other service providers: We may share Service Data or Customer Information with third party vendors, consultants and other service providers who are working on our behalf and with whom the sharing of such information is necessary to undertake that work, for example, to provide customer support. Prior to sharing data with a provider, Sift assesses the provider's security controls to ensure the data is adequately protected. Sift requires that any information disclosed to a provider is used only to provide services to Sift and only as allowed by applicable law.

Data enrichment: We may share minimal Service Data (e.g. email addresses) with select third-party service providers for data enrichment purposes. Enriching data allows us to provide a richer subset of data from which to make more informed fraud risk assessments. For example, we may work with providers that match publicly-available information from social media with Users' email addresses provided to us. Prior to sharing data with any data enrichment provider, Sift assesses the provider's security controls to ensure the data is adequately protected. Sift requires that any information disclosed to a provider is used only to provide services to Sift and only as allowed by applicable law.

Compliance with laws: We may disclose Service Data or Customer Information to a third party where we are legally required to do so in order to comply with any applicable law, regulation, legal process or government request.

Vital interests and legal rights: We may disclose Service Data or Customer Information if we believe it necessary to protect the vital interests or legal rights of Sift, our Customers or the rights or property of others.

Corporate Affiliates and Transactions: We may provide Service Data or Customer Information to our affiliates (meaning any subsidiary, parent company or company under common control with Sift). Our affiliates will use such information only as described in this Notice. Additionally, if Sift is involved in a merger, acquisition or sale of all or a portion of its assets, Customer Information and Service Data may be shared or transferred as part of that transaction, as permitted by law.

Security Safeguards

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

For the latest information about the controls we have in place to safeguard customer information, view our [Security and Privacy Overview](#).

PART V. YOUR PRIVACY

If your personal information is included in the Service Data or Customer Information, the following terms apply to you:

Update and access to your information

You may request access to your information to review, modify or request deletion of any personal information we process about you. We will review your request and will respond in accordance with our standard policies and applicable data protection laws. To protect your privacy and security, we take reasonable steps to verify the requestor's identity before processing rights requests.

Unsubscribe from our mailing list

You may at any time ask us to stop sending marketing communications to you, including by visiting this [link](#) or clicking "Unsubscribe" in any marketing e-mail communications we send you. If you have any questions relating to the "Unsubscribe" process, please let us know via the contact details set out below.

PART VI. ADDITIONAL INFORMATION FOR EEA RESIDENTS

In addition to the above described terms, if you are accessing Customer Sites from the European Economic Area (EEA), the following terms apply:

Your Privacy Rights

Objecting to processing of, or requesting restriction or portability of, personal information

If you are a resident of the EEA, you can object to processing of your personal information, ask us to restrict processing of your personal information or, if applicable, request the portability of your personal information. You can send an email to privacy@siftscience.com to exercise these rights.

Right to complain to a data protection authority

If you are a resident in the EEA, you have the legal right to complain to a data protection authorities in the EEA about Sift's collection and use of their personal information. For more information, please contact your local data protection authority. Contact details for data protection authorities in the EEA are available [here](#).

Processing of information in the U.S.

While you may access the Customer Sites from outside of the United States, the Service Data provided to Sift by its Customers is transferred to and hosted on Sift's servers in the United States. Additionally, Sift may use third-party service providers and partners in the United States and globally. The United States has data protection laws that are different than the laws of your country. 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 collected in the EEA, when that personal information is transferred to our servers in the United States for processing, we comply with the EU-US and Swiss-US Privacy Shield Frameworks as set forth by the US Department of Commerce. 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 will govern.

Legal Basis

With respect to personal information collected in the EEA and included in the Service Data, we rely on our legitimate business interests to process that personal information for the purposes described in this Notice. Our legitimate interests include: (1) fraud prevention for the benefit of Sift and its Customers; (2) maintaining, developing and improving the Sift Service; and (3) measuring the effectiveness of the Sift Service.

Data retention

We retain personal information included in the Service Data where we have an ongoing legitimate business need to do so (for example, to continue to provide fraud prevention products and services). While retaining the data, we will securely store personal information and ensure third-parties use strong security safeguards. Over time, Sift may no longer have an ongoing legitimate business need to process applicable personal information. At that time, we will either delete the data or anonymize it.

PART VII. CHANGES AND HOW TO CONTACT SIFT

Changes to this Notice

We may revise this Notice from time to time. If we do so, we will update the "Last Updated" date above. Customers and Users should revisit this page to stay aware of any changes. If we make any material changes to this Notice, we will post the updated version here and notify Users by means of a prominent notice on our website.

How to Contact Sift

You can contact Sift and its Privacy Officer with any questions or comments about this Notice or our privacy practices by email at privacy@siftscience.com or in writing to:

Sift Science, Inc.
Attn: Privacy Officer
123 Mission Street, 20th Floor
San Francisco, CA 94105

If you are located in the EEA, Sift Science, Inc. is the data controller of personal information collected through its Service.

Privacy Resources

[Site Privacy Policy](#)

[Privacy Shield Notice](#)

[Security and Privacy Overview](#)

COMPANY

[ABOUT US](#)

[CAREERS](#)

[CONTACT US](#)

[NEWS & PRESS](#)

[PARTNER WITH US](#)

[BLOG](#)

SUPPORT

[HELP CENTER](#)

[CONTACT SUPPORT](#)

[SYSTEM STATUS](#)

[TRUST & SAFETY EDU](#)

DEVELOPERS

[OVERVIEW](#)

[APIS](#)

[CLIENT LIBRARIES](#)

[INTEGRATION GUIDES](#)

[TUTORIALS](#)

[ENGINEERING BLOG](#)

SOCIAL

Don't miss a thing

Our newsletter delivers industry trends, insights, and more.

Email Address

Email

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.

© 2020 Sift All Rights Reserved

PRIVACY & TERMS