

Affinity Solutions Privacy Policy

Introduction

Affinity Solutions, Inc. (“**Affinity**”, “**we**”, “**us**”, “**our**”) is a provider of technology, analytics, data-processing, and business services for our customers (“**Customers**”). Our primary focus is running reward programs (i.e., point-accrual or cash-back programs) that bring value to the relationship between a payment-card holder and their issuing financial institution (“**FI**”) (such as a bank or credit union).

We take the protection of personal information very seriously. Please read this privacy policy (the “**Policy**”) to learn what we are doing with personal information, how we protect it, and what privacy rights you may have under applicable data protection and state privacy laws.

This Privacy Policy was last updated on 8/15/2024

Printable .pdf version of this Policy may be obtained [here](#).

What is covered by this Privacy Policy?

This Policy addresses individual consumers (“**Consumers**”) whose personal information we may receive from our FI Customers or our business partners as part of providing services to our FI Customers (the “**Services**”). We do not decide what personal information is being processed, and in general we will only access such personal information at our FI Customer’s request in connection with FI Customer support or account administration matters. We will only access such personal information to provide the Services that our FI Customer has directed us to provide, or if we are required to do so by law.

When you give your personal information to one of our FI Customers or when we collect your personal information on *their* behalf, our FI Customer’s privacy policy, rather than this policy, will apply to our processing of your personal information. If you have a direct relationship with one of our FI Customers, please contact them to exercise your privacy rights.

This Policy also covers Consumers whose personal information we:

- receive directly through other means, such as our website(s);
- receive from our business partners for the purposes of providing Services to our Customers who are not FIs (the “**Non-FI Customers**”);
- process to promote our products and services.

Affinity's primary business is in the U.S.; but we also operate in the U.K. Accordingly, the vast majority of the personal information we process concerns U.S. Consumers and business contacts. To the extent we process "personal data" for our business in the U.K., such processing is limited to data collected through our website and the personal information of our business contacts. Any services we offer in the U.K. rely exclusively on data that does not contain any personal information (and therefore no longer constitutes "personal data") in accordance with U.K. law.

Our Role with Respect to Your Personal Information

We maintain information that (i.e., that does not relate to an identified or identifiable consumer and generally cannot be used for reidentification). Accordingly, it falls outside of the scope of many data-privacy laws, such as the CCPA, CPRA, and the UK GDPR, and is not considered "personal information" or "personal data" under this Policy.

This includes data sets we derive from information that we receive from our customers and business partners on topics such as consumer financial transactions and television viewership habits. It also includes certain data products that Affinity produces and sells, which provide insights into consumer and retailer behaviors.

Because this information is considered "blind", under GLBA, you do not have the same rights with regard to it that you have regarding your personal information. Affinity also cannot respond to individualized requests regarding blinded data because we have no way to trace that data to Consumers.

What Is Not Covered by this Privacy Policy?

If you are an employee, or an applicant for employment, please refer to our Employee Privacy Policy for information concerning our collection and use of employment related personal information.

What is in this Policy?

This Policy tells you, among other things:

- our role with respect to your personal information;
- what personal information we process and how we obtain it;
- the lawful bases for processing personal information;
- our purposes of processing personal information;
- how long we keep personal information;
- how we disclose personal information;
- your privacy rights and how to exercise those rights;
- how we protect personal information; and
- how to contact us.

Our Role with Respect to Your Personal Information

We process certain personal information for our own purposes and other personal information on behalf of our Customers.

- Regarding the personal information of our website users or business contacts and prospects of Affinity, we decide the purposes and means of processing, and consequently act as a CCPA regulated “business” or data controller in accordance with the UK GDPR.
- Regarding the personal information of any individuals whose personal information is processed on behalf of our FI Customers, we process personal information as a CCPA regulated “service provider” on behalf of our FI Customers, who use our Services to operate rewards programs (i.e., point-accrual or cash-back programs).
- Regarding the personal information of any individuals whose personal information we process for our own purposes, for example in order to offer our Services to our Non-FI Customers, we decide the purposes and means of processing, and consequently act as a CCPA regulated business or data controller in accordance with the UK GDPR.

Our Basis for Processing

When we act as a data controller, we may process your personal information based on:

- your consent;
- the need to perform a contract with you;
- our legitimate interests (such as our need to improve our products and Services, conduct business with our customers and partners, and market our Services) or the legitimate interests of a third party;
- the need to comply with the law; or
- any other ground, as required or permitted by law.

Where we process your personal information based on your consent, you may withdraw it at any time. However, this will not affect the lawfulness of our processing before you withdrew your consent. It will also not affect the validity of our processing of personal information performed on other lawful grounds. We generally do not base our processing of personal information on consent.

Where we receive your personal information as part of providing our Services to you to fulfill a contract, we require such personal information to be able to carry out the contract. Without that necessary personal information, we will not be able to provide the Services to you.

Within the scope of this Policy, we may also process personal information based on the instructions of our FI Customers. To learn about their lawful bases for processing your personal information, please read the privacy policy (s) of our relevant FI Customers, such as your bank or credit union.

What Personal Information We Process and How We Obtain It

The table below describes the categories of personal information we have collected about you in the last twelve months.

Personal Information We Collect, Process, or Store	How We Obtain It
<p style="text-align: center;"><i>Identifiers</i></p> <p>Name, postal address, email address, account name, Internet Protocol address, email address, or other similar identifiers.</p>	<ul style="list-style-type: none"> • Our Customers or business partners (including their employees, contractors, and other representatives of their companies) provide it to us; • You, as a representative of one of our Customers, give it directly to us for the purposes of sales or Customer support; • You visit our websites and social media sites; or • Our vendors provide it to us.
<p style="text-align: center;"><i>Protected characteristics.</i></p> <p>Age, gender, marital status.</p>	<ul style="list-style-type: none"> • Our vendors provide it to us.
<p style="text-align: center;"><i>Other Personal Information</i></p> <p>Bank account number, credit card number, debit card number, or other financial information.</p>	<ul style="list-style-type: none"> • Our Customers or business partners (including their employees, contractors, and other representatives of their companies) provide it to us; or • Our vendors provide it to us.
<p style="text-align: center;"><i>Commercial information</i></p> <p>Products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</p>	<ul style="list-style-type: none"> • Our Customers or business partners (including their employees, contractors, and other representatives of their companies) provide it to us; or • Our vendors provide it to us.
<p style="text-align: center;"><i>Internet or other similar network activity</i></p> <p>Information about your interactions with our website.</p>	<ul style="list-style-type: none"> • You visit our websites and social media sites.
<p style="text-align: center;"><i>Geolocation information</i></p>	<ul style="list-style-type: none"> • Our Customers or business partners (including their employees, contractors,

Physical location (based on internet activity or financial transaction information).	<p>and other representatives of their companies) provide it to us;</p> <ul style="list-style-type: none"> • You visit our websites and social media sites; or • Our vendors provide it to us.
<p><i>Professional or employment-related information</i></p> <p>Current or past job history, job title.</p>	<ul style="list-style-type: none"> • Our Customers or business partners (including their employees, contractors, and other representatives of their companies) provide it to us; or • You, as a representative of one of our Customers, give it directly to us for the purposes of sales or Customer support.
<p><i>Inferences drawn from other personal information.</i></p> <p>Profile reflecting a Consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.</p>	<ul style="list-style-type: none"> • Prepared using internal analysis of other categories of personal information.

Cookies

A “cookie” is a small file stored on your device that contains information about your device. We may use cookies to provide basic relevant ads, website functionality, authentication (session management), usage analytics (web analytics), to remember your settings, and to generally improve our websites.

We may use session and persistent cookies. Session cookies are deleted when you close your browser. Persistent cookies may remain even after you close your browser, but always have an expiration date. Most of the cookies placed on your device through our Services are first-party cookies, which are placed directly by us. Other parties, such as Google, may also set their own (third-party) cookies through our websites. Please refer to the policies of these third parties to learn more about the way in which they collect and process information about you.

If you would prefer not to accept cookies, you can change the settings of your browser to reject all or some cookies. Note, if you reject certain cookies, you may not be able to use all features of our websites. For more information, please visit <https://www.aboutcookies.org/>.

Purposes of Processing Personal Information

We may process your personal information for the following purposes:

- working with our Customers and business partners;
- managing our Customer base;
- providing Services as specified in applicable contracts with our Customers;
- operating our websites, including maintaining their integrity and security;
- responding to your requests or questions;
- fulfilling our legal obligations and enforcing our rights;
- ensuring the quality of our products and Services; and
- detecting and preventing any security threats, fraud, or other criminal or malicious activity.

As a service provider to FIs, use of personal information provided to us by our FI Customers is limited to supporting and delivering the FI-branded reward program services, as specified in contracts with Affinity's FI Customers and business partners. These FI reward program services may include:

- sending emails with reward program offers to card holders;
- hosting websites to deliver reward program offers;
- authenticating reward program members when they interact with offers;
- processing transaction data to determine point or cash-back awards;
- analyzing merchant data to identify transactions occurring at specific retailers;
- conducting data analysis to match specific retailer offers to card holders to improve card holder relevance;
- conducting data analysis to create reward-program experiences (such as timely messaging and/or experiential benefits) that are highly relevant and appealing to card holders; and
- appending third-party data (e.g., demographics) to cardholder records to further improve the relevance and appeal of retailer offers.

Affinity does not use personal information provided by FIs for any purpose other than directly providing the contracted, financial institution-branded, reward program services.

How Long We Keep Personal Information

We will retain your personal information for as long as is necessary to fulfill the purpose for which we collected your personal information and any other permitted purpose, in compliance with our data retention policies. For example, we will retain and use your personal information to the extent necessary to comply with our legal obligations (e.g., if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

In cases where we act as a service provider, we retain personal information for as long as instructed by the respective Customer (who typically acts as a data controller).

Your personal information may need to be retained in our backup systems consistent with industry practice. This may be the case even when you or a Supervisory Authority has validly asked us to delete your personal information or when we no longer have a legal basis for processing such personal information. If you have requested that we delete your personal information, we will make reasonable efforts to delete any of your information restored from backup after we have processed your request.

Disclosing Personal Information to Third Parties

The following table describes, in the last twelve months, the categories of information we have disclosed to third parties for business purposes, and the categories of those third parties.

The only personal information we sell concerning Consumers is demographic information (e.g., age, income, education level) that we obtain from third-party vendors, as well as insights or propensity scores that we append to that information (i.e., inferences drawn from other personal information). This information is sold or licensed to business partners to build profiles of aggregated groups of consumers to characterize purchase behavior. We also provide personal information to third party marketing partners for use in marketing solutions they provide to their customers.

Personal Information Disclosed for Business Purposes		
Category	Yes or No	Categories of Third Parties Receiving Personal Information
<i>Identifiers</i>	Yes	<ul style="list-style-type: none"> ● Customers, business partners and marketing partners; ● Service providers who support our rewards programs; ● Email service providers; and ● Web analytics providers.
<i>Protected characteristics</i>	Yes	<ul style="list-style-type: none"> ● Customers, business partners and marketing partners.
<i>Other personal information</i>	Yes	<ul style="list-style-type: none"> ● Customers, business partners and marketing partners;

		<ul style="list-style-type: none"> • Service providers who support our rewards programs.
<i>Commercial information</i>	Yes	<ul style="list-style-type: none"> • Customers, business partners and marketing partners • Service providers who support our rewards programs; and • Retailers and merchants.
<i>Internet or similar network activity</i>	Yes	<ul style="list-style-type: none"> • Web analytics providers.
<i>Geolocation information</i>	Yes	<ul style="list-style-type: none"> • Customers, business partners and marketing partners • Service providers who support our rewards programs; • Web analytics providers.
<i>Professional or employment-related information</i>	No	<ul style="list-style-type: none"> • N/A.
<i>Inferences drawn from other personal information</i>	Yes	<ul style="list-style-type: none"> • Customers, business partners and marketing partners; and • Retailers and merchants.

Other Disclosures of Your Personal Information

We may disclose your personal information to the extent required by law, or if we have a good-faith belief that we need to disclose it in order to comply with official investigations or legal proceedings (whether initiated by governmental/law enforcement officials, or private parties). If we must disclose your personal information to governmental/law enforcement officials, we may not be able to ensure that those officials will maintain the privacy and security of your personal information.

We may also disclose your personal information if we sell or transfer all or some of our company's business interests, assets, or both, or in connection with a corporate restructuring. Finally, we may disclose your personal information to our subsidiaries

or affiliates, but only if necessary for business purposes, as described in the section above.

We reserve the right to use, transfer, sell, and disclose aggregated, privacy enhanced data for any legal purpose. Such data does not include any personal information. The purposes may include analyzing usage trends or seeking compatible advertisers, sponsors, and customers.

What Privacy Rights Do You Have?

Subject to applicable law and depending on where you reside, you may have rights regarding your personal information that we collect and process. Please note that you can only exercise these rights with respect to personal information that we process about you when we act as a data controller or as a “business” under the CCPA. To exercise your rights with respect to information processed by us on behalf of one of our Customers, please read the privacy policy of that Customer, such as your bank or credit union.

In this section, we describe those rights and explain how you can exercise those rights.

The right to be informed.

It means that you may have the right to obtain from us information regarding our processing activities that concern you, such as how we collect and use your personal information, how long we will keep it, and who it will be shared with, among other things.

We are informing you of how we process your personal information with this Policy.

The right of access.

This right may allow you to ask for details of the personal information we hold about you.

You may have the right to obtain from us confirmation of whether or not we process personal information concerning you and, where that is the case, a copy of or access to the personal information and certain related information.

Once we receive and confirm that a qualifying request came from you or your authorized agent, we will disclose to you, when requested:

- The categories of your personal information that we process;
- The categories of sources for your personal information;
- Our purposes for processing your personal information;

- Where possible, the retention period for your personal information, or, if not possible, the criteria used to determine the retention period;
- The categories of third parties with whom we share your personal information;
- If we carry out certain types of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you;
- The specific pieces of personal information that we process concerning you;
- The personal information that you have provided to us, if any, in an easily sharable format;
- If we sold or disclosed your personal information for a business purpose, the categories of personal information and categories of recipients of that personal information for both sale and disclosure;
- If we rely on legitimate interests as a lawful basis to process your personal information, the specific legitimate interests; and
- The appropriate safeguards used to transfer personal data from the UK to a third country, if applicable.

Under some circumstances, we may deny your access request. In that event, we will respond to you with the reason for the denial.

CCPA does not allow us to disclose Social Security numbers, driver's license numbers or other government-issued identification numbers, financial account numbers, any health insurance or medical identification numbers, account passwords, or security questions and answers. We can inform you that we have this information generally, but we may not provide the specific numbers, passwords, etc. to you for security and legal reasons.

Right to Correct inaccurate Personal Information

It may give you the right to ask us to correct without undue delay things that you think are wrong with the personal information we have on file about you, and to complete any incomplete personal information.

If you believe your personal information is inaccurate, please contact us and we will do our best to correct the personal information for you.

The right to erasure, right to deletion, or the right to be forgotten.

This right means you may be able to ask for your personal information to be deleted.

Sometimes we can delete your information, but other times it is not possible for either technical or legal reasons. If that is the case, we will consider if we can limit how we use it. We will also inform you of our reason for denying your deletion request.

The right to restrict processing

This is the right to ask us to only use or store your personal information for certain purposes. You may have this right in certain instances, such as where you believe the data is inaccurate or the processing activity is unlawful.

The right to object

This is the right to tell us to stop using your personal information. You may have this right where we rely on a legitimate interest of ours (or of a third party). You may also object at any time to the processing of your personal information for our direct marketing purposes. Affinity generally does not engage in direct marketing to Consumers, however.

In response to a valid objection, we will stop processing the relevant personal information unless: (i) we have compelling legitimate grounds for the processing that override your interests, rights, or freedoms; or (ii) we need to continue processing your personal information to establish, exercise, or defend a legal claim.

The right to data portability.

It is the right to ask for and receive a portable copy of your personal information that you have given us or that you have generated by using our services. Generally, Affinity does not receive data from Consumers that gives rise to a right to portability. In response to a valid request, we will provide this personal information in a structured, commonly used, and machine-readable format. When you request this information electronically, we will provide you with a copy in electronic format.

Right Related to Automated Decision Making

We sometimes use computers to study your personal information. For decisions that may seriously impact you, you have the right not to be subject to the sole use of automatic decision-making. But in those cases, we will explain to you when we might do this, why, and the effect. Generally, Affinity does not engage in this type of automated decision making.

Right to Withdraw Your Consent

Where we rely on your consent as the legal basis for processing your personal information, you may be able to withdraw your consent at any time. If you withdraw your consent, our use of your personal information before you withdraw is still lawful. Generally, Affinity does not base its processing of personal information on consent.

If you have given consent for your information to be shared with a third party and wish to withdraw this consent, please also contact the relevant third party in order to change your preferences.

Right to Non-Discrimination

As required by law, Affinity will not discriminate against you for exercising any of your privacy rights.

Your Right to Opt-Out

You may have the right to ask us to not sell your personal information, referred to as the right to opt-out.

How Can You Exercise Your Privacy Rights?

To exercise any of the rights described above, please submit a request by either:

1. **(RECOMMENDED)** Filling out [this online form](#).

2. **(Alternative) Mailing** us at:

Affinity Solutions, Inc.
Attn: Privacy Officer
112 West 34th Street, 18th Floor
New York, NY 10120

3. **Via Toll-Free Number:** 877-218-7776

Authentication of Your Identity

in order to correctly respond to your privacy rights requests, we may need to confirm that you made the request. Consequently, we may require additional information to authenticate your identity. We will authenticate your identity by asking you to provide or confirm certain information that we already hold about you. We will only use the personal information you provide to us in a request to authenticate your identity or authority to make the request. Also, when we respond, applicable law may not allow us to disclose Social Security numbers, driver's license numbers or other government-issued identification numbers, financial account numbers, any health insurance or medical identification numbers, account passwords, or security questions and answers. We can inform you that we have this information generally, but we may not provide the specific numbers, passwords, etc. to you for security and legal reasons.

Verification of Authority

If you are submitting a request on behalf of somebody else, we will need to verify your authority to act on behalf of that individual. When contacting us, please provide us with proof that the individual gave you signed permission to submit this request, a valid power of attorney on behalf of the individual, or proof of parental responsibility or legal guardianship. Alternatively, you may ask the individual to directly contact us to authenticate their identity with Affinity and confirm that they gave you permission to submit the request.

Response Timing and Format of Our Responses

We will generally confirm the receipt of your request within ten (10) business days, and in that communication, we will also describe how we will authenticate your identity (if needed) and when you should expect a response, unless we have already granted or denied the request.

Please allow us up to forty-five (45) days to reply to your requests (except requests to stop selling your personal information) from the day we receive your request. If we need more time (up to 90 days in total), we will inform you of the reason why and the extension period in writing. For requests from UK residents, please allow us up to one month to reply to your requests, which may be extend to up to three months if necessary. If we need an extension, we will provide the reason why and the extension period in writing.

We will generally act upon your request to opt-out from selling your personal information within fifteen (15) business days. We will also notify the third parties to whom we sold your personal information of your request and instruct them not to further sell your personal information. We will inform you about this within ninety (90) days from receipt of your request.

If we cannot satisfy a request, we will explain why in our response.

We will usually not charge a fee for processing or responding to your requests. However, we may charge a fee if we determine that your request is excessive, repetitive, or manifestly unfounded. In those cases, we will tell you why we made that determination and provide you with a cost estimate before completing your request.

Privacy of Children

Our website is not intended for use by those under the age of 18, nor is it targeted to those under the age of 18. We do not knowingly collect, sell or share personal information from those under the age of 16 online. If you are under the age of 16, we ask that you do not provide any information on our website through any of its features, and promptly discontinue use of our website. If we become aware that we have collected personal information from children without verification of any required parental consent, we will take steps to remove that personal information from our servers.

Data Integrity & Security

We are strongly committed to keeping your personal information safe. We have implemented and will maintain technical, administrative, and physical safeguards that are reasonably designed to help protect your personal information from unauthorized processing. Unauthorized processing includes unauthorized access, exfiltration, theft, disclosure, alteration, or destruction. Some of those measures include encryption and redaction and we also have dedicated personnel to look after information security and privacy.

We protect personal information and other data with strict security standards and a robust company-wide security program that is fully integrated and supported at all levels of the company.

We are PCI DSS Level 1 certified by independent audit. We are also SSAE 18 SOC 1 and SOC 2 audited by an independent third party for secure operation controls, and we routinely participate in audits with Affinity's FI Customers and partners to ensure that all Consumer personal information is protected and used only for approved purposes. Our personnel are regularly trained on security measures as well as privacy protection guidelines.

We keep a watchful eye on legal developments to ensure that we are compliant with the laws and regulations that protect privacy, and we provide Consumers with transparent disclosures, including describing Consumer rights.

Data Request Statistics

Under applicable law, we are required to provide you with notice concerning the number of data requests received and, of those requests, how many were complied with and denied. We provide that information in the chart below:

CCPA Reporting Requirements	Metrics for 2023
Total Volume of Requests to Know Received	1
Number of Requests to Know Fulfilled	0
Number of Requests to Know Denied	1
Median Number of Days to Respond to Requests to Know	1
Mean Number of Days to Respond to Requests to Know	1
Total Volume of Requests to Delete Received	
Total Volume of Requests to Delete Received	8
Number of Requests to Delete Fulfilled	0
Number of Requests to Delete Denied	0
Number of Requests denied as not being verifiable	8
Number of Requests denied that were not made by a consumer	0
Number of Requests that called for information exempt from deletion	0
Number of Requests denied on other grounds	0
Median Number of Days to Respond to Requests to Delete (includes 45 Day Extensions)	1
Mean Number of Days to Respond to Requests to Delete	1
Number of requests in which deletion was not required in whole, or in part, under each provision in California Civil Code section 1798.145 or 1798.146.	0
Total Volume of Requests to Limit Use of Sensitive Personal Information Received	
Total Volume of Requests to Limit Use of Sensitive Personal Information Received	0
Number of Requests to Limit Use of Sensitive Personal Information Fulfilled	0
Number of Requests to Limit Use of Sensitive Personal Information Denied*	0
Median Number of Days to Respond to Requests to Limit Use of Sensitive Personal Information	0
Mean Number of Days to Respond to Requests to Limit Use of Sensitive Personal Information	0
Total Volume of Requests to Correction Received	
Total Volume of Requests to Correction Received	0
Number of Requests to Correction Fulfilled	0
Number of Requests to Correction Denied*	0
Median Number of Days to Respond to Requests to Correction	0
Mean Number of Days to Respond to Requests to Correction	0

Total Volume of Requests to Opt-Out Received	63
Number of Opt-Out Requests Fulfilled	0
Number of Opt-Out Requests Denied	0
Median Number of Days to Respond to Requests to Opt-Out	1
Mean Number of Days to Respond to Requests to Opt-Out	1

Changes to this Policy

If we make any material change to this Policy, we will post the revised Policy to this page and update the “Effective” date.

Contact Us

If you have any questions about this Policy, please contact us by Toll Free Phone at 877-218-7776 or by postal mail at:

Affinity Solutions, Inc.

Attn: Privacy Officer
112 West 34th Street, 18th Floor
New York, NY 10120

United Kingdom Representative

We have appointed [VeraSafe](#) as our representative in the UK for data protection matters. While you may also contact us, VeraSafe can be contacted on matters related to the processing of personal data. VeraSafe can be contacted by using [this contact form](#), by telephone at +44 (20) 4532 2003, or by postal mail at:

VeraSafe United Kingdom Ltd.

37 Albert Embankment
London SE1 7TL
United Kingdom

In the U.K., if you have a complaint about how we process your personal data, which is generally made up of B2B Information, you can contact the U.K.’s Information Commissioner’s Office [here](#).