**DRAFT**

**PERSONAL & CONFIDENTIAL**

**ATTORNEY-CLIENT COMMUNICATION**

**California Privacy Policy**

Last Updated: **[insert date]**

**Scott Fetzer Company [Fillin in division]** and its subsidiaries and affiliated companies (“**Company**”) takes your privacy seriously. We want you to know how we collect, use, disclose, and retain your personal information.

**Assistance For The Disabled**

Alternative formats of this Privacy Policy are available to individuals with a disability. Please contact **privacy@scottfetzer.com**for assistance.

**This Privacy Policy explains**:

1. What categories of personal information we collect
2. The categories of sources from which we collect this personal information
3. The purposes for which we use your personal information
4. How we may disclose your personal information
5. How long we keep your personal information
6. Privacy rights for California residents
7. Changes to this Privacy Policy

**CHILDREN’S ONLINE PRIVACY PROTECTION ACT COMPLIANCE**

We do not collect information from anyone under 13 years of age. The products and/or services we provide, together with our Site, are all directed to individuals who are at least 13 years old. If you are under the age of 13, you are not authorized to use our services or the Site.

**Scope**

This Privacy Policy applies to the personal information of individuals (“**you**”, “**your**”, or “**yours**”) collected by Company, including the personal information collected when you visit our websites [www.adalet.com](http://www.adalet.com) or [www.enclosurehub.com](http://www.enclosurehub.com) as it may be modified, relocated and/or redirected from time to time (the “**Site**”). This Privacy Policy does not apply to the personal information of individuals in their capacity as prospective, current, or former employees, contract workers, board members, or owners of **Company**, or their emergency contacts, dependents, or beneficiaries.

“**Personal information**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

**Other web sites**

The Site may contain links to other web sites not operated or controlled by use (“**Third Party Sites**”). The policies and procedures we describe here do not apply to Third Party Sites. The links from the Site do not imply that we endorse or have reviewed the Third Party Sites. We suggest contacting those sites directly for information on their privacy policies.

[**DRAFTING NOTE**: Please review the factual descriptions in the Sections below to ensure that they accurately reflect Company’s practices.

Note on “categories”: With the exception of Section 3 (purposes), each of the Sections 1-4 below is only required to cover categories rather than an exhaustive list. Therefore, Company should focus on ensuring that the categories adequately cover the personal information collected, sources, etc., and add and delete categories as needed. Although the examples within each category need not be exhaustive, Company should review to ensure that they give consumers a good sense of what the category covers and do not include examples inapplicable to Company. For example, if Company does not and will not use surveillance cameras, then it should delete “footage from video surveillance cameras” from the list below to avoid potentially alarming consumers. However, the list of purposes should be exhaustive. Please review to ensure that the list of purposes covers all the purposes for which Company has used personal information in the last 12 months or plans to use personal information. **PLEASE DELETE THIS NOTE BEFORE FINALIZING**.]

1. **WHAT CATEGORIES OF PERSONAL INFORMATION WE COLLECT**
2. **Identifiers**, for example: real name, alias, telephone number, postal address, e-mail address, signature, photographs, and Social Security, driver’s license, or state identification card.
3. **Commercial Information**, for example: records of products or services purchased, [warranty registrations,] and purchasing or consuming histories.
4. **Internet Activity Information**, for example: information about your usage of the Site, such as the pages you viewed, the services and features you used or interacted with; your browser type and details about any links or communications with which you interacted; internet protocol (IP); browser plug-in types and versions; and operating systems and platform.
5. **Professional Information**, for example: business contact information and title.
6. **Financial Information**, for example: payment card details, billing address, and shipping address.
7. **Sensory or Surveillance Data**, for example: voicemails and recordings as described below in “User Content”.
8. **User Content**, includes content you submit when you contact customer service or otherwise contact Company. This may include recordings you create, including audio recordings or voicemail you submit in connection with customer service.
9. **Communications Data**, for example: during our communications with you, we collect the content of these communications as well as metadata about the communications, *i.e.*, date and time of the call or text (SMS or MMS) message and phone numbers.
10. **Geolocation data**, for example: certain features in our services/platform may collect your precise location information if you grant permission to do so in your device settings.
11. **Inferences**, for example: Company might infer based on your purchase history that you would be interested in other products or services.

**[DRAFTING NOTE**: Please review the protected categories below with particular care. **PLEASE DELETE THIS NOTE BEFORE FINALIZING]**

1. **Characteristics of Protected Classifications Under California or Federal Law**, for example: your age or gender.

**Note on Sensitive Personal Information:** Company does not infer characteristics from sensitive personal information. Company only uses sensitive personal information as necessary to perform the services or provide the goods the average person would reasonably expect when requesting those goods or services, to ensure security and integrity, short term transient use, to maintain the quality of our products and services, or for other purposes permitted by the California Privacy Rights Act and implementing regulations (“**CPRA**”) without the right to opt out.

**[DRAFTING NOTE ON SENSITIVE PERSONAL INFORMATION**: Please delete the “Note on Sensitive Personal Information” above if not accurate.

The CPRA requires additional compliance obligations if a business collects or uses sensitive personal information for “the purpose of inferring characteristics” about the individual. For example, a business might use an individual’s precise geolocation data to draw inferences about their household income or spending habits.

In that case, the company must provide specific disclosures about its collection, use, and retention of sensitive personal information. Moreover, the CPRA gives individuals the right to demand that the business restrict uses and disclosures of sensitive personal information to (a) uses and disclosures necessary to perform the services or provide the goods the average person would reasonably expect when requesting those goods or services and (b) certain purposes specified in the CPRA, e.g., data security, physical safety, preventing fraud or illegal actions, short-term transient use, quality control, uses required by law, and disclosures to vendors in support of permitted purposes.

“Infer” is defined as “the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.” “Characteristics” is not defined. This leaves ambiguity about what it means to “infer characteristics.” The CPRA’s final regulations may provide more clarity on this point.

“Sensitive personal information” is the following:

* Social Security, driver's license, state identification card, or passport number;
* account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
* precise geolocation;
* racial or ethnic origin, religious or philosophical beliefs, or union membership;
* contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;
* genetic data;
* biometric information processed for the purpose of uniquely identifying a California resident;
* personal information collected and analyzed concerning a California resident's health; and
* personal information collected and analyzed concerning a California resident's sex life or sexual orientation.

**PLEASE DELETE THIS NOTE BEFORE FINALIZING]**

**Do We Use Cookies?**

Yes. Cookies are small files that the Site or our service provider transfers to your computer’s hard drive through your Web browser that enables the Site’s or service provider’s systems to recognize your browser and capture and remember certain information. We use cookies to help us understand how users use the Site. For example, cookies gather information about how long you spend on a web page so that we can understand what web pages are of most interest to users.

If you prefer, you can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off cookies by adjusting your browser settings. If you turn off your cookies, some of the features on the Site may not function properly.

**Google Analytics**

We use cookies provided by Google Analytics, a third-party service provider, to assist us in better understanding our Site visitors. These cookies collect data tied to a user’s IP address, such as the length of time a user spends on a page, the pages a user visits, and the websites a user visits before and after visiting the Site. Based on this information, Google Analytics compiles aggregate data about Site traffic and Site interactions, which we use to offer better Site experiences and tools in the future. Google Analytics does not collect any personal information (other than IP Address which may be considered personal information in some countries). For more information on Google Analytics, visit <https://support.google.com/analytics>. [**DRAFTING NOTE**: Please delete this section if not applicable. If this section is applicable, please note that the California Attorney General’s settlement with Sephora for violations of the California Consumer Privacy Act indicates that the California Attorney General is taking the position that using services like Google Analytics may result in a “sale” of personal information to a third party. To reduce this risk, the Company should consider analytics providers that are willing to sign agreements that comply with the CPRA’s service provider requirements under Cal. Civ. Code §§ 1798.100(d), 140(ag).]

**Web Beacons**

We include small graphic images or other web programming code, called web beacons (also known as "pixel tags", “web bugs” or "clear GIFs"), on the Site. The web beacons are minute graphics with a unique identifier. They are used to track the online movements of Web users. In contrast to cookies, which are stored in a user's computer hard drive, web beacons are embedded invisibly on Web pages and are about the size of the period at the end of this sentence. Rejecting cookies using browser settings may not stop web beacons from tracking you. [**DRAFTING NOTE**: Please delete this section if not applicable and please consider the note above regarding service provider agreements.]

**Tracking Across Time and Different Sites**

The Site [tracks/does not track] your online activities over time and across websites or online services on an individually identifiable basis. [For example, we may serve you advertisements on other websites based on what appeared to interest you on our Site.] We [do/do not] allow third parties to use our Site to track your activities over time or across other websites.

**Do Not Track Setting**

The Site currently [responds/does not respond] to web browser “do not track” (DNT) signals or other mechanisms that indicate your preference for having information collected over time and across different web sites following your visit to our Site. DNT is a preference you can set in your browser’s settings to let the website you visit, including the Site, know that you do not want the websites collecting your personal identifiable information. You can also visit <https://allaboutdnt.com/> to learn more.

1. **THE CATEGORIES OF SOURCES FROM WHICH WE COLLECT YOUR PERSONAL INFORMATION**
* **You**, for example, when you register with our Site, subscribe to online services, when you shop with us, or when you otherwise provide information directly to us.
* **Service providers**, for example, analytics providers, IT, and system administration services.
* **Affiliated companies**, for example, so that we can assist other companies in The Scott Fetzer Company family of companies in providing you with products or services.
* **Automated technologies**, for example, browsing activity collected by automated technologies on the Site.
* **Third parties**, for example, lawyers, bankers, auditors, and insurers who provide consultancy, banking, legal, insurance, and accounting services.
* **Public sources**, for example, public databases.
* **Marketing/advertising companies**, for example, from social media platforms, consumer research companies, and analytics or marketing/advertising companies.
* **Surveillance/recording technologies installed by Company**, for example, video surveillance in common areas of Company facilities, voicemail technologies, and audio recording technologies with consent to the extent required by law.
* **Government or administrative agencies**, for example, law enforcement, public health officials, and other government authorities.
* **Acquired entity**, if Company acquired another entity, Company might collect personal information from that entity.
* **Other sources**, for example, [**insert other categories of sources as appropriate**.]
1. **THE PURPOSES FOR WHICH WE USE YOUR PERSONAL INFORMATION**

**Providing Products and Services, including:**

* To deliver our products and administer our services.
* To communicate with you.
* To improve our products and services, develop new products and services, and conduct research on further improvements.
* To enhance your experience using our products and services and to personalize your online experience.

**Support and Marketing, including:**

* For customer support.
* To respond to any requests, queries, suggestions, feedback, or comments you may have.
* Where you have agreed to receive such information, to send you marketing information about our products and services, including notifying you of marketing events, membership and rewards programs, promotions, and sweepstakes.
* To inform you of any changes to the services, your account (if applicable), this Privacy Policy, or any other policies or terms in relation thereto.
* To perform operations to maintain the services, including to conduct data analysis, testing, and research; and to monitor and analyze usage and activity trends.

**Monitoring, Security, and Compliance, including:**

* To administer and protect our business and our Site (including troubleshooting, analysis, testing, system maintenance, support, reporting and hosting of data, and preventing fraud and abuse).
* To store, host, or backup (whether for disaster recovery or otherwise) our services or any data contained therein.
* To protect the rights, property, or safety of Company, you, or others.
* In connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of Company or any of its subsidiaries or affiliates.
* To report suspected criminal conduct to law enforcement and cooperate in investigations.
* To exercise Company’s rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel.
* To ensure compliance with applicable laws and regulatory obligations.

**Incidental Purposes:** Any incidental purposes related to, or in connection with, the above.

**Anticipated Purposes of Use:** Although Company has not used personal information for the following purposes in the past 12 months, it may do so in the future:

* [**DRAFTING NOTE:** Insert here new purposes of use that you anticipate and that have not applied in the last 12 months. For example, if Company is planning to introduce a website feature that would use personal information for new purposes, then that should be addressed here. If Company does not plan to use personal information differently, you can delete this “Anticipated Purposes of Use” section. **PLEASE DELETE THIS NOTE PRIOR TO FINALIZING THE POLICY.**]
1. **HOW WE MAY DISCLOSE YOUR PERSONAL INFORMATION**

Company discloses personal information as necessary for the purposes described in Section 3 above to the following categories of external recipients:

* **Service providers and contractors**: Company discloses your personal information to service providers and contractors for the purposes above to assist us in meeting our business needs and contractual and legal obligations.
	+ Company only discloses your personal information to service providers and contractors subject to written contracts under Company’s direction and instructions as required by applicable law.
	+ Service providers and contractors include auditors, administrative service providers, law firms, and any other entity providing services to Company.
* **Affiliated companies**: Other companies within The Scott Fetzer Company family, for example, to provide you with our products and services.
* **Government or administrative agencies**: For example, Company may report unlawful activity to law enforcement. We may disclose information requested by government or administrative agencies including law enforcement.
* **Public**: Company may disclose personal information to the public as part of a press release, for example, to announce the winner of a sweepstakes if required by state law.
* **Required Disclosures:** We may be required to disclose personal information in a court proceeding, in response to a court order, subpoena, civil discovery request, other legal process, or as otherwise required by law.
* **Legal Compliance and Protections:** We may disclose personal information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of Company, our users, or others.
* **Corporate Transactions**: We reserve the right to disclose and transfer your personal information, including your personal information:
	+ To a subsequent owner or co-owner.
	+ In connection with a corporate merger, consolidation, bankruptcy, the sale of substantially all of our membership interests and/or assets or other corporate change, including to any prospective purchasers.

**We do not sell your personal information or disclose it to third parties for cross-context behavioral advertising.** We also do not sell the personal information of children under 16 nor disclose it to third parties for cross-context behavioral advertising.

**Aggregated and Deidentified Information**

We may aggregate and/or deidentify information, use it internally, and disclose to third parties. Neither Aggregated Information nor Deidentified Information (defined below) is personal information.

* “**Aggregated Information**” refers to information about a group of individuals from which the individually identifiable information has been removed. An example of Aggregated Information would be the statistic that 20 people used our website’s contact form on a given day.
* “**Deidentified Information**” means information subjected to reasonable measures to ensure that the deidentified information cannot be associated with the individual. An example of Deidentified Information would be data point that an unidentified visitor first entered the Site through our main web page. We maintain Deidentified Information in a deidentified form and do not attempt to reidentify it, except that we may attempt to reidentify the information just to determine whether our deidentification processes function correctly. [**DRAFTING NOTE**: The CPRA requires that a business take the measures described in this paragraph to deidentify personal information. In addition, the business must “publicly commit” to refrain from re-identifying the data, which is why we have included this section. The CPRA also requires the business to contractually obligates any recipients of the deidentified information to comply with the points above. Otherwise, the information is not “deidentified” as defined by the CPRA. **PLEASE DELETE THIS NOTE PRIOR TO FINALIZING THE POLICY.**]
1. **HOW LONG WE KEEP YOUR PERSONAL INFORMATION**

We retain your personal information for the duration of the customer relationship, if any. We also retain your personal information for 12 months after our last interaction with you. We will retain personal information longer as necessary to comply with legal, administrative, or procedural requirements, for example, a litigation hold.\

We retain your information during the time we have an ongoing relationship with you. Our internal uses and retention for personal information varies by department and certain business units. We retain your information as reasonably necessary and proportionate to the purpose for which each category of information was collected and will be processed. Records, or portions thereof may be deleted when there is no longer a legal, compliance, or business purpose to retain your information. We retain all personal information for at least 3 years and can retain certain information for as long as 10 years, which may be longer depending on the circumstances.

[**DRAFTING NOTE**: The CPRA requires that the notice at collection explain “[t]he length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period.” We have suggested language above. Company should revise in accordance with its consumer/customer data retention schedule. **PLEASE DELETE THIS NOTE PRIOR TO FINALIZING THE POLICY**.]

1. **PRIVACY RIGHTS FOR CALIFORNIA RESIDENTS**
2. **Your California Privacy Rights**

Subject to applicable law, California residents have the following rights:

* **Right to Know**: You have the right to submit a verifiable request for specific pieces of your personal information obtained from you and for information about Company’s collection, use, and disclosure of your personal information. Please note that the CPRA’s right to obtain “specific pieces” does not grant a right to the whole of any document that contains personal information, but only to copies of items of personal information. Moreover, California residents generally just have a right to know categories, for example, categories of third parties to which personal information is disclosed, but not the individual third parties.
* **Right to Delete**: You have the right to submit a verifiable request for the deletion of personal information that you have provided to Company.
* **Right to Correct**: You have the right to submit a verifiable request for the correction of inaccurate personal information maintained by Company, taking into account the nature of the personal information and the purposes of processing the personal information.
* **Right to Restrict Use and Disclosure of Sensitive Personal information**: You have the right to restrict Company’s use and disclosure of your sensitive personal information to purposes permitted under the CPRA, such as security, quality control, uses required by law, and disclosures to vendors in support of the permitted purposes. This right only applies to sensitive personal information collected or processed by Company for the purpose of inferring characteristics about you.
1. **How to Exercise Your Rights**

Company will respond to requests to know, delete, and correct in accordance with applicable law if it can verify the identity of the individual submitting the request. You can exercise these rights in the following ways:

* Call 1-888-811-005

* Privacy@scottfetzer.com or complete the request form available here [**insert link to form**].

To restrict the use and disclosure of your sensitive personal information to permitted purposes, click here: **Limit the Use of My Sensitive Personal Information**

[**DRAFTING NOTE**: You can delete the sentence above if Company (a) does not “infer characteristics” from sensitive personal information or (b) only uses sensitive personal information for the CPRA’s limited purposes. For more information on sensitive personal information, please refer to the “Drafting Note on Sensitive Personal Information” above.

If Company must include this section, then the draft CPRA Regulations also require that this link be located at either the header or the footer of the business’s internet homepages. **PLEASE DELETE THIS NOTE BEFORE FINALIZING**]

1. **How We Will Verify Your Request**

If you submit a request through a password-protected account that you created before the date of your request, we will use the authentication mechanisms in the account to verify your identity. Otherwise, we match personal data that you provide us against personal data we maintain in our files. The more risk entailed by the request (e.g., a request for specific pieces of personal data), the more items of personal data we may request to verify you. If we cannot verify your identity to a sufficient level of certainty to respond to your request, we will let you know promptly and explain why we cannot verify your identity.

1. **Authorized Agents**

If an authorized agent submits a request to know, correct, or delete on your behalf, the authorized agent must submit with the request either (a) a power of attorney that is valid under California law, or (b) document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you to follow the applicable process described above for verifying your identity. You can obtain an “Authorized Agent Designation” form by contacting us at privacy@scottfetzer.com.

1. **Company’s Non-Discrimination Policy**

Company will not unlawfully discriminate against you for exercising your privacy rights under the California Privacy Rights Act.

1. **Disclosures for Direct Marketing Purposes**

California consumers who use the services may request that we provide certain information regarding our disclosure of your personal information to third parties for their direct marketing purposes. You can make such a request by e-mail to [**insert email address**].

1. **Notice of Financial Incentives**

**[DRAFTING NOTE:** If the Company provides California residents with a “financial incentive”, then it must provide a notice about that financial incentive. This notice need not be in the privacy policy, but it might be convenient to include it here. “Financial incentive” means a program, benefit, or other offering, including payments to California residents, for the collection, retention, sale, or sharing of personal information. Price or service differences are types of financial incentives. **PLEASE DELETE THIS NOTE BEFORE FINALIZING**]

1. **CHANGES TO THIS PRIVACY POLICY**

If we change this Privacy Policy, we will post those changes on this page and update the Privacy Policy modification date above. If we materially change this Privacy Policy in a way that affects how we use or disclose your personal information, we will provide a prominent notice of such changes and the effective date of the changes before making them.

**For More Information**

For questions or concerns about Company’s privacy policies and practices, please contact us at [**insert e-mail address**].