

California Personnel Consumer Privacy Act Notice at Collection

Seen Finance, Inc., (“Seen”) collects, maintains and uses personal information about those we employ, including employees, job applicants, owners, officers, and independent contractors (“Personnel”), and those we interact with in our business-to-business relationships (“B2B Contacts”) who are California residents. Seen provides this Notice at Collection (“Notice”) to inform you about the categories of personal information to be collected and the purposes for which the categories of personal information will be used as a Seen Personnel and B2B Contacts. Please see Seen’s Online Privacy Policy at: <https://seen.com/legal/privacy-policy> for more information about our privacy practices including any applicable privacy rights that may be available.

Whether your Information is Sold or Shared

We do not sell your personal information or sensitive personal information. We may share your personal information and sensitive personal information with Seen’s third-party employment-related service providers, such as recruiters, payroll agencies, health insurance and other benefits providers, equity management companies, retirement plan providers and advisors, and other such providers. We may share your internet and other electronic network activities with our advertising partners as that term is defined under applicable law for cross-context behavioral advertising.

Retention Period

We will retain your information for the duration of your engagement with us, and for a limited period thereafter as necessary and pursuant to our internal data retention policy. We will not retain your personal information or sensitive personal information for longer than is reasonably necessary for the purposes disclosed in this Notice.

If you would like a copy of this Notice mailed, e-mailed or faxed to you, please contact us at legal@seen.com or you may request an alternative format by contacting a Customer Service Representative at (833) 923-7336.

Categories of Personal Information	Examples	Business/Commercial Purpose for which Personal Information is Collected and Used
Identifiers	Real name, alias, postal address, unique personal identifier, online identifier, Internet protocol address, email address, Social Security number, driver’s license number, passport number, or other similar identifiers, etc.	Performing human resource functions on behalf of the business or service provider, including maintaining or servicing information collected and used in an employment context, providing employee/job applicant/contractor services, processing and administering

<p>Characteristics of protected classifications under California or federal law</p>	<p>Family Information (marital status, relevant information on spouse/dependents); benefit information (wellness information, COBRA information, healthcare plan information, disability insurance and life insurance information); disability claims records (workers' compensation records and disability claims records); medical reports or records (pre-employment drug tests, medical benefits-related documentation); physical characteristics (age, disability, race, color, gender), etc.</p>	<p>benefits, verifying employee/job applicant/contractor information, processing payroll, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.</p> <p>Auditing related to a current interaction with the employee/job applicant/contractor and concurrent transactions, and auditing compliance with this specification and other standards.</p>
<p>Professional or employment-related information</p>	<p>Employment history, employment verification, promotions, service dates, training information, length of service, compensation, tax information, bank account data, current department/position, employment status, job performance, disciplinary documents, recordings of customer servicing calls, relocation information, employee development information, payroll information, etc.</p>	<p>Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.</p> <p>Debugging to identify and repair errors that impair existing intended functionality.</p>
<p>Education Information</p>	<p>Education reimbursement information, resume and application information, education verification, etc.</p>	<p>Undertaking internal research for technological development and demonstration.</p>
<p>Commercial Information</p>	<p>Products or services we have provided to you or other purchasing or consuming histories or tendencies.</p>	<p>Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the</p>
<p>Inferences</p>	<p>Job related information (job performance, disciplinary documents, employee development information), etc.</p>	<p>Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the</p>

Internet or other electronic network activity information	Job related information (web tracking, sites visited, login information, etc.); how you use our website, browsing history, search history, and any other information regarding your interaction with our website or advertisements, etc.	service or device that is owned, manufactured, manufactured for, or controlled by the business. Comply with federal, state, or local laws.
Geolocation data	Company-issued device information, company vehicle information, etc.	Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
Audio, electronic, visual, thermal, olfactory, or similar information	Visual information (video interviews, security cameras), call recordings, etc.	Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
Categories of personal information described in the California Customer Records Statute (Col. Civ. Code §1798180(e))	Identifiers, commercial information, professional or employment-related information, medical information, health insurance information, payroll information (bank account number), insurance policy numbers, etc.	Exercise or defend legal claims.
Sensitive personal information	Social Security number, driver's license, state identification card, passport number, geolocation data, account log-in, financial account, debit card, or credit card in combination with any required security or access code, password, or credentials allowing access to an account, racial or ethnic origin, citizenship or immigration status, etc.	