



PRIVACY NOTICE

Last Updated: June 2024

Welcome to Fortegra—a global specialty insurer delivering risk management solutions that help people and businesses succeed in the face of uncertainty. This Privacy Notice provides a description of Fortegra’s privacy practices relating to the in-scope products, services and data processing identified below. However, this Privacy Notice is not a contract and does not create any legal rights or obligations not otherwise provided by law.

Scope of Privacy Notice

In-Scope Products, Services and Data Processing

This Privacy Notice explains how The Fortegra Group, Inc. and its respective business units, operating companies and subsidiaries in the United States (collectively, “**Fortegra**”, “**we**”, “**us**”, or “**our**”) collect, use, disclose, and otherwise process personal data in connection with the following products and services:

- Our corporate websites that link to this Privacy Notice;
- Our interactions with individuals acting as representatives of third-party business customers, partners, and vendors;
- Our consumer product and home protection plans and services;
- Our automotive protection plans and services; and
- Our consumer data and identity protection plans and services.

Please note not all our products and services are available in every jurisdiction and, as a result, you may not be able to access or obtain certain of our products and services where you are a resident of a restricted state. We may also choose or be required by law to provide different or additional disclosures relating to the processing of personal data about residents of certain countries, regions, or states. Please refer to the [Region-Specific Disclosures](#) section below for additional disclosures that may be applicable to you.

Out-of-Scope Products, Services and Data Processing

This Privacy Notice does not apply to or address:

- **Our Financial Products or Services:** Certain of our products and services are subject to the United States Fair Credit Reporting Act (“**FCRA**”), Gramm-Leach-Bliley Act (“**GLBA**”), and other state-specific financial privacy laws. This Privacy Notice does not address our privacy practices relating to these products and services. If you apply for or obtain a financial product or service with us, you will receive a copy of the applicable Consumer Privacy Notice, electronic copies of which are available [here](#).
- **Our Processing of Data on Behalf of Business Partners:** We may on occasion process personal data solely on behalf of our business partners or allow our business partners to process personal data about their own customers in connection with certain of our

business-related products and services. We recommend referring to the privacy notice of the business partner with which you have a relationship for information on how the business partner handles personal data or otherwise engages processors, like us, to process personal data on their behalf. In addition, we are generally not permitted to respond to individual requests relating to personal data we process on behalf of our business partners, so we recommend directing any such requests to the relevant business partner.

- **Our Employment-Related Practices:** We process personal data relating to Fortegra job applicants, employees, and other employment-related individuals. This Privacy Notice does not address our privacy practices relating to such employment-related data.
- **Data Not Subject to Applicable Data Protection Laws:** Certain types of data, including deidentified and publicly available information, are not subject to applicable data protection laws. This Privacy Notice does not address our privacy practices relating to such non-covered data.

Our Collection of Personal Data

From the first moment an individual interacts with us, we are collecting personal data about that individual. Sometimes we collect personal data automatically when an individual interacts with our services and sometimes we collect personal data directly from the individual. At times, we may also collect personal data about an individual from other sources and third parties, even before our first direct interaction.

Personal Data Provided by Individuals

We collect the following categories of personal data individuals provide:

- **Contact Information**, including first and last name, phone number, email address, mailing address, the nature of your relationship with us (including whether you are interacting with us on your own behalf or on behalf of your employer), and communication preferences.
- **Professional Information**, including job title, company name, and other professional background.
- **Account Information**, including first and last name, age, signature, alias, account name and number, email address, phone number, account credentials or one-time passcodes, and the products or services you are interested in, purchased, or have otherwise used.
- **Consumer Product and Home Protection Information**, including:
 - The plan or service purchased.
 - The scope of protections provided, and the products or property subject to protection.
 - The contract or sales invoice for the protected products or property.
 - Any claims filed (including a description of the covered damage and photo evidence), and the manner in which they were resolved (including whether the claim was approved or denied, and any money or replacement products provided).
 - The location of the product or property (when leveraging a location-based service or benefit, such as mobile device locate or tracking services).

- Security measures implemented (when leveraging a security service or benefit, such as mobile device remote lock, data wipe, or culprit photo capture).
- Any other information provided in connection with a claim or resolution.
- **Automotive Protection Information**, including:
 - The plan or service purchased.
 - The scope of protections and benefits provided, and the automobiles or property subject to protection.
 - The individuals subject to protection (including, where relevant, the individual's driver's license number).
 - The contract or sales invoice for the protected automobile or property.
 - Any claims filed (including a description of the covered event and photo evidence, where required), and the manner in which they were resolved (including whether the claim was approved or denied, and any money or replacement products or services provided).
 - The location of the automobile or occupant (when leveraging a location-based service or benefit).
 - Any other information provided in connection with a claim or resolution.
- **Consumer Data and Identity Protection Information**, including:
 - The plan or service purchased.
 - The scope of protections and benefits provided.
 - The identities of the individuals subject to protection (including Social Security number, where applicable).
 - Any claims filed (including a description of the covered event), and the manner in which they were resolved (including whether the claim was approved or denied, and any money or replacement products or services provided).
 - Any other information provided in connection with a claim or resolution.
- **Payment Information**, including debit card information, billing address, and other financial information (such as, routing and account number).

Please note that we use third-party payment processing providers to process payments made to us. We do not retain any personally identifiable financial information, such as debit card number or bank account information, you provide these third-party payment processing providers in connection with payments. Rather, all such information is provided directly by you to our third-party payment processing providers. The payment processing provider's use of your personal data is governed by their privacy notice.
- **Feedback and Support Information**, including the contents of custom messages sent through the forms, chat platforms, email addresses, or other contact information we make available to customers, as well as recordings of calls or chats with us, where permitted by law (including through the use of automated tools provided by us or our third-party providers).
- **Security-Related Information**, including name and contact information of visitors to our premises, video recordings of visitors on our premises, and electronic login records and access details when a visitor utilizes company technology on our premises.

If you choose to contact us, we may need additional information to fulfill the request or respond to your inquiry. We may provide additional privacy disclosures where the scope of the request we receive or personal data we require fall outside the scope of this Privacy Notice. In that case,

the additional privacy disclosures will govern how we may process the information you provide at that time.

Personal Data Automatically Collected

We, and our third-party partners, use automatic data collection technologies (including cookies, web beacons, pixels, embedded scripts, mobile SDKs, location-identifying technologies, and logging technologies) to automatically collect the following data when you use our services or otherwise engage with us:

- **Information About Your Device and Network**, including the device type, manufacturer, and model, operating system, IP address, browser type, Internet service provider, and unique identifiers associated with you, your device, or your network (including, for example, a persistent device identifier or advertising ID).
- **Information About the Way Individuals Use Our Services and Interact With Us**, including the browser you use, the site from which you came, the site to which you are going when you leave our services, how frequently you access our services, whether you open emails or click the links contained in emails, whether you access our services from multiple devices, and other browsing behavior and actions you take on our services (such as the pages you visit, the content you view, the communications you have through our services, the content, links and ads you interact with, and specific mouse movements, scrolling, clicks, and keystroke activity on our services).
- **Information About Your Location**, including general geographic location that we or our third-party providers may derive from your IP address, as well as more precise geolocation when you grant us access through your device settings (for example, if you use our mobile device location / tracking and automotive location / tracking services).

Information we collect automatically may be combined with other personal data we collect directly from you or receive from other sources. We may also use third-party technologies to recognize when two or more devices are likely being used by the same individual and (where permitted) to link information collected from different devices.

For information about the choices you may have in relation to our use of automatic data collection technologies, please refer to the [Your Privacy Choices](#) section below. For additional details about the cookies we use on our websites and to adjust your preferences with regard to these cookies, please visit our "Cookie Preferences" manager linked from the bottom of our website via the available cookie icon.

Personal Data from Other Sources and Third Parties

We may receive the same categories of personal data as described above from the following sources and other parties:

- **Our Affiliates:** Fortegra entities receive personal data from other Fortegra entities for purposes and uses that are consistent with this Privacy Notice.
- **Other Customers:** We may receive your personal data from our other customers, including as part of a referral or family-based protection plan.
- **Your Employer:** If you interact with us in your capacity as a representative of one of our business customers, partners, or vendors, we may obtain personal data about you from the business you represent (such as by receiving your contact information from the business you represent to allow us to communicate with you about the business's relationship with us).

- **Business Partners:** Some of our products and services are offered in connection with transactions being pursued at our business partners. As a result, we may receive certain personal data (such as the product(s) or service(s) purchased in connection with the transaction) from our business partners to help facilitate a customer's request for a product or service.
- **Social Media:** When you interact with us through social media networks, such as when you follow us or share our content on social networks, we may receive some information that you permit the social network to share with third parties. The data we receive is dependent upon your privacy settings with the social network, and may include profile information, profile picture, username, and any other information you permit the social network to share with third parties.
- **Advertisers, Influencers, and Publishers:** We engage in advertising both on our services and through third-party services. Advertisers, influencers, and publishers may share personal data with us in connection with our advertising efforts.
- **Service Providers:** Our service providers that perform services on our behalf, such as analytics and certain marketing providers, collect personal data and often share some or all of this information with us.
- **Other Sources:** We may also collect personal data about you from other sources, including publicly available sources, third-party data providers, brand partnerships, or through transactions such as mergers and acquisitions.
- **Inferences:** We may generate inferences or predictions about you and your interests and preferences based on the other personal data we collect and the interactions we have with you.

Our Use of Personal Data

We use personal data we collect to:

- Fulfill or meet the reason the information was provided, such as to fulfill our contractual obligations, to evaluate an application for a protection plan, facilitate payments, or to deliver the products and services requested;
- Manage our organization and its day-to-day operations;
- Communicate with you, including via email, text message, chat, social media and/or telephone calls;
- Facilitate the relationship we have with you and, where applicable, the business you represent;
- Request you provide us feedback about our product and service offerings;
- Address inquiries or complaints made by or about an individual in connection with our products or services;
- Create and maintain accounts for our business and individual customers;
- Verify your identity and entitlement to our products and services;
- Market our products and services to you, including through email and social media;
- Administer, improve, and personalize our products and services, including by recognizing you and remembering your information when you return to our products and services;
- Develop, operate, improve, maintain, protect, and provide the features and functionality of our products and services;

- Identify and analyze how you use our products and services;
- Infer additional information about you from your use of our products and services, such as your interests.
- Create aggregated or de-identified information that cannot reasonably be used to identify you, which information we may use for purposes outside the scope of this Privacy Notice;
- Conduct research and analytics on our customer base and our products and services, including to better understand the demographics of our users;
- Improve and customize our products and services to address the needs and interests of our user base and other individuals we interact with;
- Test, enhance, update, and monitor the products and services, or diagnose or fix technology problems;
- Help maintain and enhance the safety, security, and integrity of our property, products, services, technology, assets, and business;
- Defend, protect, or enforce our rights or applicable contracts and agreements (including for billing and collections), as well as to resolve disputes, to carry out our obligations and enforce our rights, and to protect our business interests and the interests and rights of our customers and other third parties;
- Detect, prevent, investigate, or provide notice of security incidents or other malicious, deceptive, fraudulent, or illegal activity and protect the rights and property of Fortegra and others;
- Facilitate business transactions and reorganizations impacting the structure of our business;
- Comply with contractual and legal obligations and requirements and as otherwise allowed by applicable law; or
- Fulfill any other purpose for which you provide your personal data, or for which you have otherwise consented.

Our Disclosure of Personal Data

We disclose or otherwise make available personal data in the following ways:

- **To Our Affiliates:** Fortegra entities disclose personal data to other Fortegra entities for purposes and uses that are consistent with this Privacy Notice.
- **Business Partners:** Some of our products and services are offered in connection with transactions being pursued at our business partners. As a result, we may share certain personal data (such as whether your request for a protection plan was approved) with our business partners to help facilitate the completion of your transaction.
- **To Your Employer:** If you interact with us in your capacity as a representative of one of our business customers, partners, and vendors, we may share personal data about you with the business you represent (such as by sharing information about your interactions with the business you represent relating to a product or service they are considering or have obtained).
- **To Marketing Providers:** We coordinate and share personal data with our marketing providers in order to advertise and communicate with you about the products and services we make available.

- **To Ad Networks and Advertising Partners:** We work with third-party advertising partners to deliver personalized advertising content on our services, on other websites and services, and across other devices. These parties may collect information automatically from your browser or device when you visit our websites and other services through the use of cookies and related technologies. This information is used to provide and inform targeted advertising, as well as to provide advertising-related services.
- **To Service Providers:** We engage other third parties to perform services on our behalf in connection with the uses of personal data described in the sections above. These service providers may process personal data on our behalf or have access to personal data while performing services on our behalf.
- **To Other Businesses as Needed to Provide Services:** We may share personal data with third parties you engage with through our services or as needed to fulfill a request or transaction.
- **In Connection with a Business Transaction or Reorganization:** We may take part in or be involved with a business transaction or reorganization. We may disclose, transfer, or assign personal data to a third-party during negotiation of, in connection with, or as an asset in such a business transaction or reorganization. Also, in the unlikely event of our bankruptcy, receivership, or insolvency, your personal data may be disclosed, transferred, or assigned to third parties in connection with the proceedings or disposition of our assets.
- **To Facilitate Legal Obligations and Rights or as Allowed by Applicable Law:** We may disclose personal data to third parties, such as legal advisors and law enforcement:
 - in connection with the establishment, exercise, or defense of legal claims;
 - to comply with laws or to respond to lawful requests and legal process;
 - to protect our rights and property and the rights and property of our agents, customers, and others, including to enforce our agreements, policies, and terms;
 - to detect, suppress, or prevent fraud;
 - to reduce credit risk and collect debts owed to us;
 - to protect the health and safety of us, our customers, or any person; or
 - as otherwise allowed by applicable law.
- **With Your Consent or Direction:** We may disclose your personal data to certain other third parties or publicly with your consent or direction. For example, with your permission, we may post your testimonial on our websites.

Your Privacy Choices

The following privacy choices are made available to all individuals with whom we interact. You may also have additional choices regarding your personal data depending on your location or residency. Please refer to our [Region-Specific Disclosures](#) below and our financial privacy law notices available [here](#) for information about additional privacy choices that may be available to you.

Communication Preferences

- **Email Communication Preferences:** You can stop receiving promotional email communications from us by clicking on the “unsubscribe” link provided in any of our email communications. Please note you cannot opt-out of service-related email communications (such as, account verification, transaction confirmation, or service update emails).
- **Push Notification Preferences:** To the extent certain of our services use push notifications, you can stop receiving push notifications from us by changing your preferences in your device's notification settings menu or in the applicable service-specific application. Please note we do not have any control over your device's notifications settings and are not responsible if they do not function as intended.
- **Direct Mailing Preferences:** You can stop receiving promotional direct mail communications from us by contacting us at consumerprivacy@fortegra.com. Please note this opt-out does not affect any mailings that are controlled by third parties that may feature or mention our products or services.

Withdrawing Your Consent

Where we have your consent for the processing of your personal data (e.g., when you opt in to receive certain types of marketing communications from us), you may withdraw your consent by following the instructions provided when your consent was requested or by contacting us as set forth in the [Contact Us](#) section below.

Automatic Data Collection Preferences

Certain of our services may allow you to adjust your preferences regarding our use of automatic data collection technologies. For example, there is a “Cookie Preferences” manager linked from the bottom of our website via the available cookie icon that allows you to adjust your preferences regarding certain automatic data collection technologies on our website for the specific device and browser you are using at that time (which means you will need to change your preferences on each device and browser you use to interact with our website).

Where a Fortegra-specific preference manager or privacy setting is not available, you may be able to utilize third-party tools and features to further restrict our use of automatic data collection technologies. For example:

- Most browsers allow you to change browser settings to limit automatic data collection technologies on websites.
- Most email providers allow you to prevent the automatic downloading of images in emails that may contain automatic data collection technologies.
- Many devices allow you to change your device settings to limit automatic data collection technologies for device applications.

Depending on the third-party tool or feature you use, you may not be able to block all automatic data collection technologies or you may need to update your preferences on multiple devices or browsers. We do not have any control over these third-party tools and features and are not responsible if they do not function as intended.

Targeted Advertising Preferences

We engage third parties to help us facilitate targeted advertising designed to show you personalized ads based on predictions of your preferences and interests developed using personal data we maintain and personal data our third-party partners obtain from your activity over time and across nonaffiliated websites and other services. The data we and our third-party partners use for purposes of facilitating targeted advertising, as well as to provide advertising-related services such as reporting, attribution, analytics, and market research, are primarily

collected through the use of a variety of automatic data collection technologies, including cookies, web beacons, pixels, embedded scripts, mobile SDKs, location-identifying technologies and logging technologies. We may share a common account identifier (such as a hashed email address) with our third-party advertising partners to help link the personal data we and our third-party partners collect to the same person, or otherwise target advertising to an individual on a third-party website or platform.

In addition to taking the steps set forth in the [Automatic Data Collection Preferences](#) section above, you may be able to further exercise control over the advertisements that you see by leveraging one or more targeted advertising opt-out programs. For example:

- **Device-Specific Opt-Out Programs:** Certain devices provide individuals the option to turn off targeted advertising for the entire device (such as Apple devices through their App Tracking Transparency framework or Android devices through their opt out of ads personalization feature). Please refer to your device manufacturer's user guides for additional information about implementing any available device-specific targeted advertising opt-outs.
- **Digital Advertising Alliance:** The [Digital Advertising Alliance](#) allows individuals to opt out of receiving online interest-based targeted advertisements from companies that participate in their program. Please follow the instructions at <https://optout.aboutads.info/?c=2&lang=EN> for browser-based advertising and <https://www.youradchoices.com/appchoices> for app-based advertising to opt out of targeted advertising carried out by our third-party partners and other third parties that participate in the Digital Advertising Alliance's self-regulatory program.
- **Network Advertising Initiative:** The [Network Advertising Initiative](#) similarly allows individuals to opt out of receiving online interest-based targeted advertisements from companies that participate in their program. Please follow the instructions at <https://optout.networkadvertising.org/?c=1> to opt out of browser-based targeted advertising carried out by our third-party partners and other third parties that participate in the Network Advertising Initiative's self-regulatory program.
- **Platform-Specific Opt-Out Programs:** Certain third-party platforms provide individuals the option to turn off targeted advertising for the entire platform (such as certain social media platforms). Please refer to your platform provider's user guides for additional information about implementing any available platform-specific targeted advertising opt-outs.

Please note that when you opt out of receiving interest-based advertisements through one of these programs, this does not mean you will no longer see advertisements from us or on our services. Instead, it means that the online ads you do see from relevant program participants should not be based on your interests. We are not responsible for the effectiveness of, or compliance with, any third parties' opt-out options or programs or the accuracy of their statements regarding their programs. In addition, program participants may still use automatic data collection technologies to collect information about your use of our services, including for analytics and fraud prevention as well as any other purpose permitted under the applicable advertising industry program.

Modifying or Deleting Your Personal Data

If you have any questions about reviewing, modifying, or deleting your personal data, you can contact us directly at consumerprivacy@fortegra.com. We may not be able to modify or delete your personal data in all circumstances.

Partner-Specific Preferences

Certain of our third-party providers and partners offer additional ways that you may exercise control over your personal data, or automatically impose limitations on the way we can use personal data in connection with the services they provide:

- **Device-Specific / Platform-Specific Preferences:** The device and/or platform you use to interact with us (such as your mobile device or social media provider), may provide you additional choices with regard to the data you choose to share with us. Please refer to your device or platform provider's user guides for additional information about implementing any available platform-specific targeted advertising opt-outs.
- **Google Analytics:** Google Analytics allows us to better understand how our customers interact with our services. For information on how Google Analytics collects and processes data, as well as how you can control information sent to Google, review Google's website here: www.google.com/policies/privacy/partners/. You can learn about Google Analytics' currently available opt-outs, including the Google Analytics Browser Add-On, here: <https://tools.google.com/dlpage/gaoptout/>.

Children's Personal Data

Our products and services are not directed to, and we do not intend to, or knowingly, collect or solicit personal data from children under the age of 13. If an individual is under the age of 13, they should not use our products and services or otherwise provide us with any personal data either directly or by other means. If a child under the age of 13 has provided personal data to us, we encourage the child's parent or guardian to contact us to request that we remove the personal data from our systems. If we learn that any personal data we collect has been provided by a child under the age of 13, we will promptly delete that personal data.

Investor Personal Data

In addition to the personal data practices outlined above, we also collect personal data from shareholders and investors of our company, including share purchasing history, number of shares held, value of the shares, and the holder of record's name and address. We use this information primarily to manage investor relations and investments in our company, including by providing you information about our company and related investments, processing investment transactions, preparing tax returns and other investor-related documents, and managing our cap table. We may also use this information for the purposes set forth in the [Our Use of Personal Data](#) section above and disclose this information to third parties in furtherance of these purposes as set forth in the [Our Disclosure of Personal Data](#) section above, as permitted by law.

Security of Personal Data

We have implemented reasonable physical, technical, and organizational safeguards that are designed to protect your personal data. In addition, we take steps designed to ensure any third party with whom we share personal data provides a similar level of protection. However, despite these controls, we cannot completely ensure or warrant the security of your personal data.

Retention of Personal Data

We will usually retain the personal data we collect about you for no longer than reasonably necessary to fulfil the purposes for which it was collected, and in accordance with our legitimate business interests and applicable law. However, if necessary, we may retain personal data for longer periods of time as required under applicable law or as needed to resolve disputes or protect our legal rights.

Once retention of the personal data is no longer reasonably necessary for the purposes outlined above, we will either delete or deidentify the personal data or, if that is not possible (for example,

because personal data has been stored in backup archives), we will securely store the personal data and isolate it from further active processing until deletion or deidentification is possible.

Third-Party Websites and Services

Our services may include links to third-party websites, plug-ins, applications and other services. Except where we post, link to or expressly adopt or refer to this Privacy Notice, this Privacy Notice does not apply to any personal data practices of third parties. To learn about the personal data practices of third parties, please visit their respective privacy notices.

Region-Specific Disclosures

We may choose or be required by law to provide different or additional disclosures relating to the processing of personal data about residents of certain countries, regions or states. If you are a resident of the states of California, Colorado Connecticut, Nevada, Oregon, Texas, Utah, or Virginia, please click [here](#) for additional state-specific privacy disclosures, including a description of the personal data rights made available to residents of these states under applicable law.

Updates to This Privacy Notice

We may update this Privacy Notice from time to time. When we make changes to this Privacy Notice, we will change the date at the beginning of this Privacy Notice. If we make material changes to this Privacy Notice, we will provide you notice as required by law using your email address, by prominently posting on this website or our other platforms, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided.

Contact Us

If you have any questions or requests in connection with this Privacy Notice or other privacy-related matters, please do not hesitate to contact us at:

Phone: 800.888.2738

Email: consumerprivacy@fortegra.com

Postal Address:

Fortegra

10751 Deerwood Park Blvd.

Ste. 200

Jacksonville, FL 32256

ADDITIONAL UNITED STATES PRIVACY DISCLOSURES

These disclosures supplement the information contained in our [Privacy Notice](#) by providing additional information about our personal data processing practices relating to individual residents of certain states in the United States. For a detailed description of how we collect, use, disclose, and otherwise process personal data, please read our [Privacy Notice](#). Please note not all our products and services are available in every jurisdiction and, as a result, you may not be able to access or obtain certain of our products and services where you are a resident of a restricted state.

Nevada Residents

If you are a resident of the state of Nevada in the United States, you have the right to opt out of the sale of your personal data. You may submit a request to opt-out of the sale of your personal data by emailing us at consumerprivacy@fortegra.com.

California, Colorado, Connecticut, Oregon, Texas, Utah, and Virginia Residents

If you are a resident of the state of California, Colorado, Connecticut, Oregon, Texas, Utah, or Virginia in the United States, the following supplementary disclosures may apply to you.

Personal Data Disclosures, Sales, and Targeted Advertising

We disclose all of the categories of personal data we collect to the categories of recipients set forth in the [Our Disclosure of Personal Data](#) section of our [Privacy Notice](#).

Our disclosure or making available of commercial information (including the products or services you are interested in, purchased, or have otherwise used), information about your device and network, information about the way in which you use our services and interact with us, and inferences about your interests and preferences to ad networks and advertising partners may qualify as the sale of personal data or the sharing or processing of personal data for the purpose of displaying advertisements that are selected based on personal data obtained or inferred over time from an individual's activities across businesses or distinctly-branded websites, applications, or other services (otherwise known as "targeted advertising" or "cross-context behavioral advertising") under certain privacy laws.

Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to limit or opt-out of the sale of personal data or the processing of personal data for purposes of targeted advertising (as described in the [Your Additional U.S. Privacy Choices](#) section below).

Please note we do not sell the personal data of individuals we know to be less than 16 years of age or share such information for targeted advertising purposes.

Sensitive Personal Data

The following personal data elements we collect may be classified as "sensitive" under certain privacy laws:

- Account credentials or one-time passcodes.
- Financial account and debit card information.
- Precise geolocation.

We only use or disclose sensitive personal data where reasonably necessary and proportionate for the purposes of providing products and performing services you have requested, verifying and improving the products and services we provide, detecting security incidents, fraud, and other illegal actions, ensuring the physical safety of natural persons, performing services on behalf of the business, or short-term transient use. We only collect and process sensitive personal data without the purpose of inferring characteristics about the relevant individual, and

we do not sell sensitive personal data or process or otherwise share sensitive personal data for the purpose of targeted advertising.

Deidentified Information

We may at times receive, or process personal data to create, deidentified information that can no longer reasonably be used to infer information about, or otherwise be linked to, a particular individual or household. Where we maintain deidentified information, we will maintain and use the information in deidentified form and not attempt to reidentify the information except as required or permitted by law.

Automated Decision-Making and Profiling

We do not conduct automated processing of personal data for the purposes of evaluating, analyzing, or predicting an individual's personal aspects in furtherance of decisions that produce legal or similarly significant effects. As a result, we do not provide a right to exercise control over such forms of automated decision-making and profiling.

Your Additional U.S. Privacy Choices

Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to exercise some or all of the following rights:

- **Right to Know:** The right to confirm whether we are processing personal data about you and, under California and Oregon law only, to obtain certain personalized details about the personal data we have collected about you, including:
 - The categories of personal data collected;
 - The categories of sources of the personal data;
 - The purposes for which the personal data were collected;
 - The categories of personal data disclosed to third parties (if any), and the categories of recipients to whom this personal data were disclosed;
 - The categories of personal data shared for targeted advertising purposes (if any), and the categories of recipients to whom the personal data were disclosed for these purposes;
 - The categories of personal data sold (if any) and the categories of third parties to whom the personal data were sold; and
 - For Oregon residents only, a list of specific third parties to whom personal data have been disclosed.
- **Right to Access & Portability:** The right to obtain access to the personal data we have collected about you and, where required by law, the right to obtain a copy of the personal data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
- **Right to Correction:** The right to correct inaccuracies in your personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.
- **Right to Control Over Sensitive Personal Data:** The right to exercise control over our collection and processing of certain sensitive personal data.
- **Right to Opt-Out of Targeted Advertising:** The right to direct us not to use or share personal data for certain targeted advertising purposes.

- **Right to Opt-Out of Sales:** The right to direct us not to sell personal data to third parties, including the right to opt-out of the disclosure of personal data to third parties for the third parties' direct marketing purposes under California's "Shine the Light" Law.
- **Right to Deletion:** The right to have us delete personal data we maintain about you.

Depending on your state of residency, you may also have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights.

Submitting Privacy Rights Requests

Please submit a request specifying the right you wish to exercise by:

- Completing our online form found [here](#); or
- Calling our toll-free U.S. telephone number: 800.888.2738.

To exercise your right to opt-out as it relates to the use of cookies and related technologies that involve the sale of personal data or the use of personal data for targeted advertising purposes, please click the available cookie icon in the bottom of the website to open our "Cookie Preferences" manager and adjust your preferences accordingly. If you are visiting our site with the Global Privacy Control enabled, any cookies that constitute sales or are used for targeted advertising should already be turned off automatically in our cookie preference manager. Please note this opt-out tool is website, device, and browser specific, so you will need to change your preferences on each website and on each device and browser you use to interact with our website. In addition, you can also opt-out of cookie-based sales by businesses that participate in the Digital Advertising Alliance's CCPA Opt-Out Tool by visiting <https://www.privacyrights.info/>. Lastly, you may follow the other steps set forth in the [Automatic Data Collection Preferences](#) and [Targeted Advertising Preferences](#) sections of the [Your Privacy Choices](#) section of our [Privacy Notice](#) to further exercise control over automatic data collection technologies.

Before processing your request to exercise certain rights (including the Right to Know, Access & Portability, Correction, and Deletion), we will need to verify your identity and confirm you are a resident of a state that offers the requested right(s). In order to verify your identity, we will generally either require the successful authentication of your account, or the matching of sufficient information you provide us to the information we maintain about you in our systems. In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or where you are not a resident of one of the eligible states.

Submitting Authorized Agent Requests

In certain circumstances, you are permitted to use an authorized agent to submit requests on your behalf through the designated methods set forth above where we can verify the authorized agent's authority to act on your behalf. In order to verify the authorized agent's authority, we generally require evidence of either (i) a valid power of attorney or (ii) a signed letter containing your name and contact information, the name and contact information of the authorized agent, and a statement of authorization for the request. Depending on the evidence provided and your state of residency, we may still need to separately reach out to you to confirm the authorized agent has permission to act on your behalf and to verify your identity in connection with the request.

Appealing Privacy Rights Decisions

Depending on your state of residency, you may be able to appeal a decision we have made in connection with your privacy rights request. All appeal requests should be submitted by replying to the communication resolving your original request.

Additional California-Specific Disclosures

The following disclosures only apply to residents of the State of California.

California Categories of Personal Data

California law requires we provide disclosures to you about what personal data we collect by reference to the enumerated categories of personal data set forth within California law. To address this obligation, we have identified the relevant enumerated California personal data category for the personal data described in the [Our Collection of Personal Data](#) section of our [Privacy Notice](#) below:

- **Identifiers**, such as first and last name, alias, account name and number, and driver's license number.
- **Customer records**, such as account name and number, account credentials or one-time passcodes, signature, phone number, email address, mailing address, the nature of your relationship with us (including whether you are interacting with us on your own behalf or on behalf of your employer), security-related information and communication preferences.
- **Protected classification characteristics**, such as age.
- **Commercial information**, such as consumer product and home protection information, automotive protection information, consumer data and identity protection information, and the other products or services you are interested in, purchased, or have otherwise used.
- **Internet / network information**, such as information about your device and network and information about the way in which you use our services and interact with us.
- **Geolocation data**, such as general geographic location derived from IP address, as well as more precise geolocation when you grant us access through your device settings (for example, if you use our mobile device location / tracking and automotive location / tracking services).
- **Sensory information**, such as recordings of calls or chats with us, or video recordings of visitors on our premises (where permitted by law).
- **Professional / employment information**, such as job title, company name, and other professional background.
- **Sensitive personal data**, such as government ID numbers (including driver's license numbers), account credentials or one-time passcodes, financial account and debit card information, and precise geolocation information.
- **Other personal data**, such as the contents of custom messages sent through the forms, chat platforms, email addresses, or other contact information we make available to.
- **Inferences**, such as predictions about you and your interests and preferences based on the other personal data we collect and the interactions we have with you.