Ouro U.S. Privacy Policy

Updated: July 31, 2025, Effective: July 31, 2025

This Privacy Policy Notice applies to Ouro Global, Inc., Ouro International, Inc., Ouro Insurance Agency, LLC, and their affiliates (collectively, "Ouro" "we" or "us"). It applies to all the products and services offered by Ouro, including on our website ("Site") and mobile application ("App") (collectively, the "Services") to U.S. consumers ("you", except where a product or service has a separate privacy notice that does not incorporate this Privacy Notice.

Ouro understands that consumers care about privacy. This Privacy Policy Notice ("Notice") describes the types of Personal Data we collect, how we use the information, with whom we may share it, and the choices available to you. We also describe measures we take to protect the security of the information and how you can contact us about our privacy practices.

When visiting or using our Sites, communicating with us electronically, interacting with us on social media or through ad content, or using a mobile App of Ouro, this Notice applies to you and governs our collection, storage, sharing, and use of your information.

If you apply for or use a Bank product serviced by Ouro or obtain an Insurer's policy procured through Ouro Insurance as agent, the Gramm-Leach-Bliley Act and State financial privacy laws govern your financial privacy rights. Therefore, if you are a customer or consumer of one of our Bank or Insurer's products (each a "Financial Product"), you should consult the privacy notice associated with that Financial Product for information on collection, storage, sharing, and use of your information. A copy of each Bank and Insurer privacy notice is distributed annually to each customer, as required by applicable law, and available online as well.

As Ouro is subject to the Gramm-Leach-Bliley Act ("GLBA"), Ouro benefits from broad exemptions under most US state privacy laws; however, California, Oregon, and Minnesota impose additional obligations for data not covered by GLBA. Specifically, while GLBA governs nonpublic Personal Data ("NPI"), these states extend privacy law coverage to other types of personal data which Ouro processes. This includes marketing data collected through tools like Google Analytics on Ouro websites, employee information, business contact data (such as contacts at retail stores, distributors, or vendors), and mobile app usage data.

Refer to State Privacy Laws to view relevant State disclosures. For California residents specifically, consumers can read our "Notice at Collection" and job applicants can read our Ouro HR Privacy Notice (for California Residents).

About Ouro & Our Provider Partners

Ouro is a financial technology company, not a bank or insurance company. Ouro is an authorized agent and program manager for Netspend® and other bank products issued by Pathward®, National Association ("Pathward"), Republic Bank & Trust Company, ("Republic"), The Bancorp Bank, N.A., ("Bancorp") and Texas First Bank ("TFB"); Members FDIC (each a "Bank"); and a licensed producer agent for the Chubb Group of Insurance Companies ("Chubb" or "Insurer") assisting individuals in the procurement of certain policy coverages.

If you are a cardholder or have applied for a card, the principal privacy notice governing your card belongs to the Bank issuing your card. Please see the back of your card or the card program marketing materials for the name of your Bank. Ouro is not responsible for our Banks' or Insurer's information practices or privacy notices. For your convenience, we provide these links below.

Bank Privacy Policies

- Privacy Notice for customers with cards issued by Pathward, National Association.
- Privacy Notice for customers with cards issued by Republic Bank & Trust Company
- Privacy Notice for customers with cards issued by The Bancorp Bank, N.A.
- Privacy Notice for customers with cards issued by Texas First Bank.

Insurer Privacy Notice

- Privacy Notice for the Chubb Group of Insurance Companies

When you visit a Site, we collect information that identifies, describes, or is reasonably capable of being associated with you ("Personal Data") and other information that does not identify you personally or contain personal identifiers ("Anonymous Information"). We define Personal Data in its broadest sense, meaning any data (such as name, contact information, social security number, etc.) that can be used to identify an individual or household, either directly or indirectly. Anonymous Information may be treated as Personal Data when it can be linked with other information to personally identify you. Personal Data does not include publicly available information, such as information lawfully made available from government records, information we have a reasonable basis to believe is lawfully made available to the general public by you or by widely distributed media, or by a person to whom you have disclosed the information and not restricted it to a specific audience, or de-identified or aggregated information.

As described below, we collect Personal Data directly from you, automatically through your use of the Sites and Services, and from third-party sources. To the extent permitted by applicable law, we may combine the information we collect from publicly available or third-party sources. The Personal Data we collect varies based on your relationship with us.

Sensitive Personal Information: Some Personal Data we may collect is defined under the law as sensitive personal information. Sensitive personal information we collect includes social security number, driver's license number, state identification card number, passport number, customer account log-in, financial account number, debit card number and credit card number in combination with any required security or access code, password, or credentials allowing access to an account, and precise geolocation information.

Consent: Our procedures ensure that your consent is reviewed, approved, and implemented appropriately across all mediums and meets the following key principles to ensure that you understand and actively agree to how your Personal Data is being used, and that you have the power to withdraw your consent at any time. These principles are:

- **Freely Given:** Consent must be obtained without coercion, pressure, or undue influence.

- **Specific and Informed:** Individuals should clearly understand what information is being collected, how it will be used, and who will have access to it.
- **Unambiguous:** Consent should be expressed in a clear and definitive manner, not through implied or ambiguous actions.
- **Affirmative Action:** Consent should require a positive action from the individual, like checking a box or clicking a button, rather than simply opting out by inaction.
- **The Right to Revoke Consent:** Individuals should have the ability to withdraw their consent at any time, with clear instructions on how to do so.

What Information is Collected

We collect information that we need to provide our Services, to administer and improve the Services, to create and offer new Services, for research purposes, and to fulfill any legal and regulatory requirements.

The Personal Data that we may collect include the following categories:

- **Identifiers**. Personal identifiers and contact information such as your name, address, email address, phone number, and other details for identity verification required for you to access our Services.
- **Government-Issued Identifiers**. Government-issued personal identifiers such as your driver's license number, social security number, or other government-issued identifiers.
- **Account Details**. Bank routing number, account number, user ID, password, and other credentials used to access our Services.
- **Payment Card Information**. Information necessary to process or verify past payments and process authorized Service transactions, including cardholder name, card number (PAN), card expiration data, card verification value, billing address, and other related information.
- **Transaction Information**. Account transaction history, direct deposit information, and information obtained with your consent about your linked non-Ouro accounts (such as transaction information and balances, payroll account information, etc.).
- **Payment Information**. If you pay a bill, we may collect information necessary to process your payment such as bank account information, billing address, and any other related information.
- **Employment information**. Employee-specific information related to payroll and health benefits, including wages and deductions including approximate or expected income and pay frequency; occupation; and income details such as employment history, references, and other information for recruiting and tracking purposes.
- **Geolocation Data**. Your IP address for identity verification and performance of Services.
- **Commercial Information**. Information about the Services you use, including interest in a Service, purchasing or consuming tendencies, and receipts or records of purchase or enrollment in other products or services.

- **Message Contents**. Messages, email contents, or any other information you choose to provide when interacting with Services, our customer service, or agents.
- **Audio or Similar Information**. Recordings of your phone conversations with our customer service team to provide or enhance Services and for quality assurance and training purposes.
- **Preferences**. Types of Services you use, your communications preferences, wish lists and other preferences you may select in your account or profile.
- **Other Information**. Responses to online forms, surveys, offerings of Service reviews; suggestions for new products or Services; participation in contests; use of self-created content such as photographs; or any other actions you perform on the Services.

Sources of Personal Data

During the 12-month period prior to the effective date of this Privacy Notice, we may have obtained Personal Data about you from the following source categories:

- Directly from you, such as when you sign up for an account, initiate a transaction, contact customer service or support departments via phone, email, chat or other forms of communication, or from applications, forms, webinars, surveys, and other information you provide us.
- Your devices, when you use our Platform or Services.
- Your comments or suggestions, interaction with us, requests for information or contact with our customer service or support departments.
- External banks (i.e., banks other than our Banks) if you link a non Ouro-serviced account.
- Vendors who provide services on our behalf.
- Our joint marketing partners.
- Our business partners (such as referring websites).
- Online advertising services and advertising networks.
- Government entities.
- Operating systems and platforms.
- Identity verification and fraud prevention platforms.
- Social networks.
- Data brokers, lead generation partners, and identity resolution service providers.
- Marketers and other websites on which Ouro advertises.
- Inferences, including new information from other data we collect, including using automated means to generate information about your likely preferences or other characteristics

("inferences"). For example, we may infer your general geographic location (such as city, state, and country) based on your IP address.

- **Information Collected by Automated Means**: We may use automated technologies on our Services to collect information about your equipment, browsing actions and usage patterns. These technologies help us (1) remember your information so you do not have to re-enter it; (2) track and understand how you use and interact with our Services, including our online forms, tools or content; (3) tailor the Services around your preferences; (4) measure the usability of our Services and the effectiveness of our communications; and (5) otherwise manage and enhance our products and Services, and help ensure they are working properly. Information collected by automated means may include:
    - Site Visitor information: When you visit our Site, we may obtain certain information by automated means, such as cookies, web beacons, web server logs and other technologies. A "cookie" is a text file that websites send to a visitor's computer or other internet-connected device to uniquely identify the visitor's browser or to store information or settings in the browser. A "web beacon," also known as an internet tag, pixel tag or clear GIF, links web pages to web servers and cookies and may be used to transmit information collected through cookies back to a web server. The information we collect in this manner may include your device IP address, unique device identifier, web browser characteristics, device characteristics, operating system, language preferences, referring URLs, clickstream data, and dates and times of website visits. Your browser may tell you how to be notified about certain types of automated collection technologies and how to restrict or disable them. Please note, however, that without these technologies, you may not be able to use all the features of our Services.

    - App User Information: When you use our App, we also may collect certain information by automated means, such as through device logs, server logs and other technologies. The information we collect in this manner may include the device type used, the mobile operating system, device identifiers and similar unique identifiers, device settings and configurations, IP addresses, battery and signal strength, usage statistics, referring emails and web addresses, dates and times of usage, actions taken on the App, and other information regarding use of the App. In addition, we may collect your device's geolocation information. Your device's operating platform may provide you with a notification when the App attempts to collect your precise geolocation. Please note that if you decline to allow the App to collect your precise geolocation, you may not be able to use all the App's features. Your device may tell you how to be notified about certain types of automated collection technologies and how to restrict or disable them. Please note, however, that without these technologies, you may not be able to use all the features of our Services. You can manage how your device and browser share certain device data by adjusting the privacy and security settings on your mobile device.

Important Note: Information collected in connection with your application or use of a particular Financial Product is covered under the applicable Bank's and Insurer's privacy notice.

Aggregated, Non-Personal, or Non-Identifiable Information

We may collect or process general, non-personal, or statistical information about the users of our Services. We may also de-identify, anonymize, and/or aggregate certain Personal Data collected from or about users of our Services, or when you interact with us. We may process and disclose this information without restriction (so long as no attempt is made to re-identify the data.

How We Collect Information

To access or use our Services, you may be required to provide Personal Data. Personal Data is primarily collected, submitted, and/or transmitted:

- When you provide it to utilize the Services or facilitate our processing of data
- From application, forms, webinars, surveys, and other information you provide us.
- If you provide us with comments or suggestions, interact with us, request information about our Services, or contact our customer service or support departments by phone, email, chat, or other forms of communication.
- From consumer and business reporting agencies regarding verification of your identity or financial accounts.
- Between us, our business partners, and third-party vendors.
- From information you may provide via social media.

We may append and enrich the information we have about you with information purchased from third party data suppliers.

We may collect both Personal Data and Anonymous Information such as connection, activity, and usage data, when visitors and users navigate to and around our Sites and Apps:

- Through your browser when you visit the Site, which includes information such as your Media Access Control (MAC) address, browser type, device type, and operating system.
- From your IP address, which is automatically logged in our server when you visit a Site.
- Using cookies or other digital tracking tools such as web beacons (also known as pixel tags or clear GIFs). See the Use of Cookies and Web Beacons section below for more information.
- From feedback that does not personally identify you voluntarily provided to us on a Site.
- Using a website recording service, which may record mouse clicks, mouse movements or page scrolling but does not record any Personal Data.
- From de-identified or aggregated Personal Data, including payment data associated with a Financial Product.

Biometric Information:

For the purposes of this Privacy Notice, “biometrics” may include an individual’s physiological characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Examples of biometrics include, but are not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted.

We do not collect biometric information, but smartphones do for access. The consent process is part of the smartphone and is controlled by the user/worker.

Data Retention:

We retain Personal Data for as long as necessary to provide the Services and fulfill the transactions requested by or on behalf of customers, or for other essential purposes such as complying with our legal obligations, maintaining business and financial records, resolving disputes, maintaining security, product development, detecting and preventing fraud and abuse, enforcing our agreements, and for any other necessary business purpose.

How We Use Your Information

Our collection of Personal Data is limited to the business and commercial purposes described below:

1. Perform services, including maintaining or servicing accounts, processing transactions, and/or other benefits, providing customer service, and other related activities ("Services").
2. Verify customers' information, identity, and eligibility to receive Services.
3. Send transactional communications as part of our Services and marketing communications that we believe may interest you.
4. Determine your eligibility for, and administer your participation in, certain features of the Services, including, but not limited to, surveys, contests, sweepstakes, promotions and rewards;
5. Conduct research, assessments, and analytics relating to our Services and develop new services, products and technological improvements.
6. Administer, audit, and improve our Platform.
7. Improve, upgrade, or enhance our Services or business operations.
8. Administer quality and safety maintenance for our Platform or Services.
9. Facilitate applicant tracking and employee recruitment.
10. Contact customers and consumers with information on Services, new Services or products, or upcoming events, including via SMS or MMS text messaging if mobile phone number is provided for that purpose and auditing those interactions.
11. Perform advanced analytics and provide insights to customers.
12. Detect fraud, theft, or other activities to ensure security and integrity by detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
13. Comply with legal, reporting, and regulatory requirements or to defend against a legal claim.
14. For other purposes that are compatible with this Privacy Policy or where permitted by applicable law.

15. In any other way we may describe when you provide the information, or for which you provide authorization.

Anonymous Information:

We may use Anonymous Information in the following ways:

- To evaluate the Site's effectiveness and usability
- To improve our products or services
- To ensure the Site displays properly and diagnose problems
- To measure the number of visitors to the Site
- For other activities to the extent permitted by law.

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated, or incompatible purposes without providing you with notice.

We Do Not Sell Your Personal Data

We do not sell Personal data for monetary or other consideration. We only make business purpose Personal data disclosures as detailed above and pursuant to written contracts that describe the purposes of use, require the recipient to keep Personal Data confidential, and prohibit using the disclosed Personal Data for any purpose except performing the contract.

How We Share the Information We Obtain

We may share the information we obtain about you with our affiliates and subsidiaries; our Banks, our Insurers; other companies in connection with co-branded products, services or programs; joint marketing partners; research study partners; and consumer reporting agencies. We also may share the information we obtain about you with vendors and other entities we engage to perform services on our behalf, such as payment and check deposit processors, risk detection and mitigation tools, and modeling and analytics tools.

We also may disclose Personal Data (1) if we are required to do so by law or legal process (such as a court order or subpoena); (2) in response to requests by government agencies, such as law enforcement authorities; (3) to establish, exercise or defend our legal rights; (4) when we believe disclosure is necessary or appropriate to prevent physical or other harm or financial loss; (5) in connection with an investigation of suspected or actual illegal activity; (6) to defend our decisions related to a dispute, which includes sharing limited dispute and decision related information, as permitted by law, with the press if the member has shared related details of the dispute with the press already; (7) in connection with the sale, transfer, merger, acquisition, joint venture, reorganization, divestiture, dissolution, or liquidation of our business or asset (disclosure associated with these events includes full transfer of your Personal Data to the resulting entitles); or (8) otherwise with your consent.

Security

We maintain organizational, technical, and physical safeguards designed to protect the Personal Data you provide against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use. SSL encryption also is used on our Site when you are asked to enter confidential information as part of your application. You can tell you have entered an encrypted session in several ways. Whenever you see an unbroken key, a locked padlock, or similar icon on your browser screen, you have entered an encrypted session. In addition, when your session changes from "http" to "https," you are in an encrypted session. More information about our online security can be found here.

Children

We do not knowingly collect or use Personal Data from children under 18 years of age without obtaining verifiable consent from their parents. We are not responsible for the data collection and use practices of non-affiliated third parties to which our Site may link.

Links to Other Websites

Our Site may include links to third-party websites. We are not responsible for the information collection practices of third-party links you click to from our Site. We cannot guarantee how these third parties use cookies or whether they place cookies on your computer that may identify you personally. We urge you to review the privacy policies of each of the linked websites you visit before you provide them with any Personal Data.

Cookies and Similar Tracking Technologies

Ouro uses cookies or other similar tracking technologies when you visit our Site. Cookies are text files containing small amounts of information, which your computer or mobile device downloads when you visit a Site. When you return to our Sites – or visit websites that use the same cookies – they recognize these cookies and therefore your browsing device.

We use cookies and other tracking technologies to do lots of different jobs, like letting you navigate between pages efficiently, remembering your preferences and generally improving your browsing experience. They can also help ensure that ads you see online are more relevant to you and your interests. We also use similar technologies such as pixel tags and JavaScript to undertake these tasks.

We use cookies to:

- Ensure your security and privacy when in our secure Sites
- Store login details for our secure sites
- Temporarily store input information in our calculators, tools, illustrations and demonstrations
- Provide you with ads that are more relevant to you and your interests, and improve our targeting and enhance your journey through our sites and partner sites
- Improve our understanding of how you navigate through our sites so we can identify improvements
- Evaluate our sites' advertising and promotional effectiveness; and
- We use both our own (first-party) and partner companies' (third-party) cookies to support these activities

We may also allow our business partners to place web beacons on our site or to place cookies on your device for advertising or other purposes.

Disabling Cookies and Do-Not-Track:

While you may disable the usage of cookies through your browser settings, we do not change our practices in response to a “Do Not Track” signal in the HTTP header from your browser or mobile application. We track your activities if you click on advertisements for Ouro services on third-party platforms such as search engines and social networks and may use analytics to track what you do in response to those advertisements. We may also use web beacons and tracking URLs in our messages to you to determine whether you have opened a certain message or accessed a certain link.

State Privacy Laws

Currently nineteen states have passed and signed privacy legislation into law. The state laws, among other provisions, provide consumers with the right to know, right to delete, right to correct, right to opt-out, and right to non-discrimination. Specific state notices are provided below.

Generally State privacy laws exclude Personal Data already covered by Federal financial services privacy laws such as the Gramm-Leach-Bliley Act (GLBA). As a result, these rights granted do not apply to Personal Data related to a financial account. However, California, Minnesota, and Oregon impose additional obligations for data not covered by GLBA. Specifically, this includes marketing data collected through prospect lists, tools like Google Analytics on Ouro websites, employee information, business contact data (such as contacts at retail stores, distributors, or vendors), and mobile app usage data.

For California Residents

Updated: July 31, 2025, Effective: July 31, 2025

The California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020 (collectively "CPRA" or “California Privacy Law”) provide consumers residing in that state ("California Consumers", "you", or "your") with specific rights regarding their Personal Data (“Personal Data”). This notice (“CPRA Privacy Notice”) supplements the information contained in the Ouro U.S. Privacy Policy (“Ouro Privacy Policy”) and explains how Ouro, and our subsidiaries and affiliates, (“Ouro,” “we,” “us,” or “our”) collect, use, disclose and retain Personal Data and how California Consumers may exercise their rights under the CPRA.

Except for those terms defined within this CPRA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the CPRA, “Personal Data” means any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. “Personal Data” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

We may collect (and may have collected during the 12-month period prior to the effective date of this Statement) the following categories of Personal Data about you:

- Identifiers. Identifiers such as a real name, signature, postal address, physical characteristics or description, unique personal identifiers (such as a device identifier; cookies, beacons, pixel tags, mobile ad identifiers and similar technology; photographs and images, customer number, unique pseudonym, or user alias; telephone number and other forms of persistent or probabilistic identifiers), online identifier, physical address, internet protocol address, email address, account name, social security number, driver's license number or state identification card number, passport number, debit card number, credit card number, or any other financial information, insurance policy number, insurance claim number, and other similar identifiers. Some Personal Data included in this category may overlap with other categories.

- Additional Data Subject to Cal. Civ. Code § 1798.80. Signature, physical characteristics or description, passport number, driver's license or other state identification card number, education, bank account number, credit card number, debit card number, and other financial information.

- Protected Classifications. Characteristics of protected classifications under California or federal law, such as race, ancestry, national origin, religion, age, sex, gender, marital status, citizenship status, military and veteran status, among others.

- Commercial Information. Commercial information, including records of personal property; products or services purchased, obtained, or considered; policy and claim information; and other purchasing or consumer histories or tendencies.

- Online Activity. Internet and other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with websites, applications or advertisements.

- Geolocation Data. We use your IP address to determine your general location (such as city, state, or zip code).

- Sensory Information. Audio, electronic, visual, and similar information.

- Employment Information. Professional or employment-related information.

- Inferences. Inferences drawn from any of the information identified above to create a profile about you reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- Sensitive Personal Data. We will not process your "Sensitive Personal Data" without your consent. Under the CPRA, Sensitive Personal Data consists of:

    - Government ID. Government identification such as social security numbers, driver's license, state identification card, or passport number.

    - Account access information. Information such as 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 data. Data derived from a device and that is used or intended to be used to locate you within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.
- Communications Content: The contents of mail, email, and text messages (unless Ouro is the intended recipient).
- Sensitive demographic data. Racial or ethnic origin, religious or philosophical beliefs, or union membership.
- Genetic Data: We do not collect or use genetic data.
- Biometric Information: We do not collect or use biometric information to uniquely identify a consumer.
- Health Information: We do not collect or use Personal Data concerning a consumer's health.
- Sex Life or Sexual Orientation: We dop not collect Personal Data concerning a consumer's sex life or sexual orientation.

Our Purposes for the Collection and Use of Personal Data:

We may collect Personal Data directly from consumers (including customers, candidates, and employees), affiliates, business partners, agents, and vendors. Our collection of Personal Data is limited to the business and commercial purposes as described below:

1. Perform services, including maintaining or servicing accounts, processing transactions, and/or other benefits, providing customer service, and other related activities (“Services”).
2. Verify customers’ information, identity, and eligibility to receive Services.
3. Send transactional communications as part of our Services and marketing communications that we believe may interest you.
4. Determine your eligibility for, and administer your participation in, certain features of the Services, including, but not limited to, surveys, contests, sweepstakes, promotions and rewards;
5. Conduct research, assessments, and analytics relating to our Services and develop new services, products and technological improvements.
6. Administer, audit, and improve our Platform.
7. Improve, upgrade, or enhance our Services or business operations.
8. Administer quality and safety maintenance for our Platform or Services.
9. Facilitate applicant tracking and employee recruitment.
10. Contact customers and consumers with information on Services, new Services or products, or upcoming events, including via SMS or MMS text messaging if mobile phone number is provided for that purpose and auditing those interactions.

11. Perform advanced analytics and provide insights to customers.
12. Detect fraud, theft, or other activities to ensure security and integrity by detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
13. Comply with legal, reporting, and regulatory requirements or to defend against a legal claim.
14. For other purposes that are compatible with this Privacy Policy or where permitted by applicable law.
15. In any other way we may describe when you provide the information, or for which you provide authorization.

We may aggregate or de-identify your Personal Data for these same purposes.

Special Notes:

Treatment of Sensitive Personal Data. You have the right to limit our processing of your "sensitive" data for the purpose of inferring characteristics about you. We may collect or process your sensitive Personal Data for the purpose of inferring characteristics about you, under the following conditions:

- only as necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
- To help ensure security and integrity to the extent the use of the consumer's Personal Data is reasonably necessary and proportionate for these purposes, such as:
    - Short term transient use as part of your current interaction with us provided that we do not disclose your Personal Data to another third party and do not build a profile about you or otherwise alter your experience outside the current interaction with the business.
    - Performing services on behalf of the business including maintaining or servicing accounts, providing customer service, processing and fulfilling orders or transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage or similar services on behalf of the business.
    - 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 service or device that is owned, manufactured, manufactured for, or controlled by the business.

Should we seek to process sensitive Personal Data for users outside these categories and to infer characteristics about you, we shall (1) provide notice to you explaining those uses and (2) allow you to opt out of those uses. If you exercise your right to limit our use our use or disclosure of your Sensitive Personal Data, we shall refrain from using or disclosing this information and wait at least twelve (12) months before requesting you again to authorize your use or disclosure of such information for additional purposes.

Sources of Personal Data:

During the 12-month period prior to the effective date of this Statement, we may have obtained Personal Data about you from the following categories of sources:

- Directly from you, such as when you sign up for an account, initiate a transaction, contact customer service or support departments via phone, email, chat or other forms of communication, or from applications, forms, webinars, surveys, and other information you provide us.
- Your devices, when you use our Platform or Services.
- Your comments or suggestions, interaction with us, requests for information or contact with our customer service or support departments.
- External banks (i.e., banks other than our Banks) if you link a non Ouro-serviced account.
- Vendors who provide services on our behalf.
- Our joint marketing partners.
- Our business partners (such as referring websites).
- Online advertising services and advertising networks.
- Government entities.
- Operating systems and platforms.
- Social networks.
- Data brokers, lead generation partners, and identity resolution service providers.

In order for us to receive your information from a lead generation partner, you must have opted-in to the partner sharing your information for direct marketing purposes or the partner may have collected your information from publicly available sources. We keep a record of your opt-in to ensure that we are not marketing to prospects without consent.

If you have received direct marketing from us, there are cases where are not able to determine a prospect's current contact information with the information provided by our lead generation partners. In those cases, we use third-party identity resolution service providers in order to verify the address and aid us in determining whether to use the lead. In the past 12 months, We have shared contact information with these third-party service providers. Our identity resolution service providers are contractually not permitted to use your information for any other purpose.

Categories of third parties with whom Personal Data was shared:

We may use, disclose, or transmit Personal Data we collect to other service providers or other third parties for business purposes, to provide our Services, or for other purposes as provided by the CPRA as described below:

A. Our affiliates, partners, or subsidiary organizations.

B. Government agencies to fulfill legal, reporting and regulatory requirements.

C. Our employees, affiliated companies, subsidiaries, contractors, agents, third-party partners including distributors and employers for payroll cards, and vendors to perform Services related

to your account, to offer additional services, perform analysis to determine qualifications to receive other services, collect amounts due, or for our business operations.

D. Third-party providers for services that you may sign up for via our Site or Services or other business partners with whom we work to develop or market certain products or services.

E. Bank partners, insurance provider partners, data, payroll, and payment processors to process transactions.

F. Cloud providers, customer management platforms, security providers, and similar services in connection with providing products, and, in the support of, our Services.

G. Law enforcement or government officials. We reserve the right to release information if we are required to do so by law or if, in our business judgment, such disclosure is reasonably necessary to comply with any court order, law, or legal process, in a fraud investigation, an audit or examination.

H. Attorneys, accountants and auditors.

I. To a buyer or successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by us is among the assets transferred.

J. Any other entity we disclose when you provide the information, or for which you provide authorization.

Categories of Personal Data Sold or Shared to Third Parties:

We do not sell Personal Data with third parties. We only make business purpose Personal Data disclosures as detailed above and pursuant to written contracts that describe the purposes of use, require the recipient to keep Personal Data confidential, and prohibit using the disclosed Personal Data for any purpose except performing the contract.

The chart below describes the categories of Personal Data collected in the previous twelve (12) months, the business or commercial purposes for such collection, and the categories of third parties with whom we may have disclosed Personal Data for a business purpose in the previous twelve (12) months:

Category of Personal Data that We May Collect and Transmit	**Examples**	**Collected During the Past 12 Months**	**Business or Commercial Purpose**	**Categories of Third Party with Whom We May Have Disclosed Personal Data During Past 12 Months**
Personal Data	Full name, address, telephone number, Social Security number, date of birth, driver's license number, passport numbers, financial, bank account,	Yes	1-15	A-J

	geolocation data, medical and beneficiary information, signatures, vaccination related information, and similar identifiers			
Sensitive Personal Data	Social Security number, driver's license, state ID card, passport number, a consumer account login, financial account, debit card or credit card number in combination with any: required security code, password, credentials allowing access to an account, a consumer's precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of: a consumer's mail, email and text messages (unless the business is the intended recipient), consumer's genetic data, processing of biometric information for the purpose of uniquely identifying a consumer, Information collected and analyzed concerning a consumers health, sex life and sexual orientation	Yes	1-4, 6-15	A-J
Protected Personal Characteristics	Age (40 years or older), race, color, ancestry, sex, gender identity, sexual orientation, national origin, marital status, veteran or military status, medical information (including medial conditions, disabilities), and similar identifiers	Yes	1-4, 6-7, 9-11, 13-15	A-D, F-J
Profession and Employment Related Information (job applicants)	Employment history, job title(s), work descriptions, locations, dates worked, performance evaluations, and similar information	Yes	9	A-D, F-J
Education Information (non-public)	Institution name, degree, GPA, years attended, professional certifications, visa sponsorship and similar information	No		

Internet and Other Electronic Identifiers	Unique user ID, browsing history, cookie data, IP address, unique device information, session logs, analytics logs, geolocation data, and similar identifiers	Yes	1-2, 5-10, 12-15	A, C-D, F-J
Inference Information	Profile reflecting preferences, characteristics or predispositions, product and service interests, order histories, search histories and similar information	Yes	1, 3-4, 6-7, 10, 14-15	A, C-D, F, I-J
Biometric Information	Iris, finger, facial scan, or voice used in the creation of identification templates for time products and voice assistance services	No		
Geolocation Data	Physical location, Device coordinates/location, or movements	Yes	1-2, 4,7-8, 14-15	A-C, G-J
Sensory Information	Images, visual, thermal, olfactory information, audio or video recordings related to the services	Yes	1,2, 4-8, 10, 12-15	A-C, G-J

California Consumer Rights under the CPRA:

As a California resident, you have rights regarding your Personal Data. Those rights and other state-specific information is described below:

- **Right to Inquire and Access**. You have to ask if we have collected Personal Data about you and to request that we disclose that Personal Data to you at no charge, twice in a 12-month period. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal Data, which is also provided in this Notice.
- **Right to Correction**. You have the right to request that we correct inaccurate Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Delete**. You have the right to request that we delete your Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Opt-Out of the Selling or Sharing of your Data, or Use of Automated Decision-Making Technology that uses Personal Data for Profiling**. You have the right to opt out of the selling or sharing of your Personal Data. The CPRA requires us to describe the categories of Personal Data we sell or share to third parties and how to opt-out of future sales. The CPRA definition of "sale" and "share" is very broad and the common flow of information for advertising and analytics may be considered a sale or sharing. Under the CPRA, Personal Data includes unique identifiers, including things like IP addresses, cookie IDs, pixel tags, and mobile ad IDs. The law defines a "sale" broadly to include simply making such Personal Data available to third parties in some

cases. “Share” is defined as providing Personal Data to a third party to target advertising to a consumer based on information about their activity on multiple websites across the internet. We do not knowingly receive monetary compensation for the sale or sharing of information to third parties; however, in the last 12 months, when you access our Services, we may let advertising and analytics providers collect IP addresses, cookie IDs, advertising IDs, and other unique identifiers, which may be collected along with device and usage data, and information about your interactions with our Services and advertisements.

- **Right to Limit Use or Disclosure of Sensitive Personal Data.** You have the right to limit our use or disclosure of Sensitive Personal Data to the following purposes (and direct our service providers, contractors, and third parties, and their business partners to do the same):
    - To provide you with the services or goods you requested;
    - To ensure security and integrity of your information;
    - To prevent, detect, and investigate security incidents that affect your information;
    - To avoid illegal actions against us and prosecute responsible parties;
    - To ensure the physical safety of persons;
    - To advertise to you during your visit to the websites linking to this Policy and other short-term uses, where your information is not disclosed to a third party or used to affect your web experience or build a consumer profile;
    - To collect or process Sensitive Personal Data for purposes other than inferring characteristics about you;
    - To maintain/service accounts, provide customer service, process payments, provide analytics, complete transactions, and perform other services on our behalf; or
    - To verify and maintain the quality or safety of, or to improve, a product or service.

  Once we receive and process your request, we will stop using and disclosing your Personal Data for purposes other than those listed above (and direct our service providers, contractors, and third parties, and their business partners to do the same).

- **Right to Non-Discrimination**. You have the right not to be discriminated against for exercising any of your privacy rights.

How to Exercise Your Privacy Rights:

California Consumers or their authorized agents may submit a request by phone at 1-866-387-7363, or by submitting a **Privacy Request Form** to us by mail at P.O. Box 2136, Austin, TX 78768-2136, or by email at privacy@ouro.com. If you’re making a request as an Authorized Agent, you must also fill out, sign and attach the **Authorized Agent Form** to your request. If the request is submitted by someone with a power of attorney (POA), the POA may be submitted instead of the Authorized Agent Form.

Authentication/Verification. To help protect your privacy and maintain security when you submit a privacy request, we are required to reasonably validate your identity. To fulfill your request, we may require you to sign a declaration under penalty of perjury that you are the consumer whose Personal Data is the subject of the request. If we cannot validate the requestor based on the information provided, we will notify the requestor that we are unable to fulfill the request. We will only use Personal Data provided in the request to verify the requestor's identity or authority to make it. We will confirm receipt of a request within ten (10) business days. We endeavor to respond to a verifiable consumer

request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period. We do not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will detail why we made that decision and provide a cost estimate before completing the request.

Declining Requests. Except for the automated controls described in this Notice, if you send us a request to exercise your rights or the choices in this section, to the extent permitted by applicable law, we may charge a fee or decline requests in certain cases. For example, we may decline requests where granting the request would be prohibited by law, could adversely affect the privacy or rights of another person, would reveal a trade secret or other confidential information, would interfere with a legal or business obligation that requires retention or use of the data, or because the data at issue is not covered under the law you are asserting.

Appeal. You have the right to appeal our decision to refuse to act on a CPRA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request. If you disagree with our explanation, you have the right to file a complaint with the State's Attorney General HERE.

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for different data types in the context of different Services, actual retention periods can vary significantly based on criteria such as user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a "financial incentive". These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

1. A succinct summary of the financial incentive or price or service difference offered;

2. A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;

3. How the consumer can opt-in to the financial incentive or price or service difference;

4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

Data Privacy Assessment. In accordance with California Privacy Law, we conduct and document a Data Protection Assessment (DPA) for various processing activities involving Personal Data. These encompass processing personal data for: targeted advertising; sale of personal data; profiling harm to consumers, or intrusion into their privacy; and managing Personal Data that poses an elevated risk of harm to consumers.

Changes to This Privacy Notice. This Notice may be revised from time to time due to legislative changes, changes in technology, our privacy practices, or new uses of your information not previously disclosed in this Policy. Revisions are effective upon posting and your continued use of this Platform or Services will indicate your acceptance of those changes. Please refer to this Policy regularly.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.

For Minnesota Residents

Updated: July 31, 2025, Effective: July 31, 2025

The Minnesota Consumer Data Protection Act (“MCDPA” or “Minnesota Privacy Law”) provides consumers residing in that state ("Minnesota Consumers", "you", or "your") with specific rights regarding their Personal Data. This notice (“MCDPA Privacy Notice”) supplements the information contained in the Ouro U.S. Privacy Policy (“Ouro Privacy Policy”) and explains how Ouro, and our subsidiaries and affiliates, (“Ouro,” “we,” “us,” or “our”) collect, use, disclose and retain Personal Data and how Minnesota Consumers may exercise their rights under the MCDPA.

Except for those terms defined within this MCDPA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the MCDPA, Personal Data means any information that can be linked to a particular natural person. “Personal data” does not include de-identified data or publicly available information.

Minnesota Privacy Law defines "Sensitive Personal Data” as a subset of Personal Data that (1) reveals racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (2) contains biometric data or genetic information for

the purpose of uniquely identifying an individual; (3) the personal data of a known child; or (4) specific geolocation data.

Minnesota Consumer Rights under the MCDPA:

If you are a Minnesota resident, you have rights regarding your Personal Data. Those rights and other state-specific information is described below:

- **Right to Inquire and Access**. You have to ask if we have collected Personal Data about you and to request that we disclose that Personal Data to you at no charge, once in a 12-month period. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal Data, which is also provided in this Notice.
- **Right to Correct**. You have the right to request that we correct inaccurate Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Delete**. You also have the right to request that we delete your Personal Data under certain circumstances, subject to a number of exceptions.
- **Right to Opt-Out of the Selling of your Data, Targeted Advertising, or Use of Automated Decision-Making Technology that uses Personal Data for Profiling**. You have the right to opt out of the sale of your Personal Data, targeted advertising and processing Personal Data for purposes of profiling. When permitted, we limit the use of profiling for marketing purposes only. Personal Data may include unique identifiers, including things like IP addresses, cookie IDs, pixel tags, and mobile ad IDs. When you access our Services, we may let advertising and analytics providers collect IP addresses, cookie IDs, advertising IDs, and other unique identifiers, which may be collected along with device and usage data, and information about your interactions with our Services and advertisements. We do not knowingly receive monetary compensation for the sale of information to third parties.
- **Right to Data Portability**. You have the right to obtain a portable copy of your Personal Data. To obtain a copy of your Personal Data that you previously provided to us in a portable format, please submit an "Access" request as described above. While these requests are distinct, we have not identified any technically feasible and readily usable format that would allow you to transmit this data to another controller. Therefore, we will provide you a copy of your Personal Data so that we honor your request as best as is technically feasible.
- **Right to Request**. You have the request a list of the specific third parties to which we have disclosed your Personal Data.
- **Right to Non-Discrimination**. You have the right not to be discriminated against for exercising any of your privacy rights.

How to Exercise Your Privacy Rights:

Minnesota Consumers or their authorized agents may submit a request by phone at 1-866-387-7363, or by submitting a **Privacy Request Form** to us by mail at P.O. Box 2136, Austin, TX 78768-2136, or by email at privacy@ouro.com. If you're making a request as an Authorized Agent, you must also fill out, sign and

attach the **Authorized Agent Form** to your request. If the request is submitted by someone with a power of attorney (POA), the POA may be submitted instead of the Authorized Agent Form.

Authentication/Verification. To help protect your privacy and maintain security when you submit a privacy request, we are required to reasonably validate your identity. To fulfill your request, we may require you to sign a declaration under penalty of perjury that you are the consumer whose Personal Data is the subject of the request. If we cannot validate the requestor based on the information provided, we will notify the requestor that we are unable to fulfill the request. We will only use Personal Data provided in the request to verify the requestor's identity or authority to make it. We will confirm receipt of a request within ten (10) business days. We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period. We do not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will detail why we made that decision and provide a cost estimate before completing the request.

Declining Requests. Except for the automated controls described in this Notice, if you send us a request to exercise your rights or the choices in this section, to the extent permitted by applicable law, we may charge a fee or decline requests in certain cases. For example, we may decline requests where granting the request would be prohibited by law, could adversely affect the privacy or rights of another person, would reveal a trade secret or other confidential information, would interfere with a legal or business obligation that requires retention or use of the data, or because the data at issue is not covered under the law you are asserting.

Appeal. You have the right to appeal our decision to refuse to act on a MCDPA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request or, if circumstances dictate, an additional 60 days' extension. If you disagree with our explanation, you have the right to file a complaint with the State's Attorney General HERE.

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for different data types in the context of different Services, actual retention periods can vary significantly based on criteria such as user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a "financial incentive". These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can

terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

1. A succinct summary of the financial incentive or price or service difference offered;

2. A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;

3. How the consumer can opt-in to the financial incentive or price or service difference;

4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.

For Oregon Residents

Updated: July 31, 2025, Effective: July 31, 2025

The Oregon Consumer Privacy Act (“OCPA” or “Oregon Privacy Law”) provides consumers residing in that state ("Oregon Consumers", "you", or "your") with specific rights regarding their Personal Data. This notice (“OCPA Privacy Notice”) supplements the information contained in the Ouro U.S. Privacy Policy (“Ouro Privacy Policy”) and explains how Ouro, and our subsidiaries and affiliates, (“Ouro,” “we,” “us,” or “our”) collect, use, disclose and retain Personal Data and how Oregon Consumers may exercise their rights under the OCPA.

Except for those terms defined within this OCPA Privacy Notice, all other capitalized terms shall have the same meaning as those designated in the Ouro Privacy Policy.

Information We Collect:

Under the OCPA, “Personal Data” means data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household. “Personal Data” does not include deidentified data or data that is lawfully available through federal, state or local government records or through widely distributed media; or a controller reasonably has understood to have been lawfully made available to the public by a consumer.

Under the OCPA, Sensitive Personal Data is information revealing racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status; is a child's personal data; accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates; or is genetic or biometric data.

How to Exercise Your Privacy Rights:

Oregon Consumers or their authorized agents may submit a request by phone at 1-866-387-7363, or by submitting a **Privacy Request Form** to us by mail at P.O. Box 2136, Austin, TX 78768-2136, or by email at privacy@ouro.com. If you're making a request as an Authorized Agent, you must also fill out, sign and attach the **Authorized Agent Form** to your request. If the request is submitted by someone with a power of attorney (POA), the POA may be submitted instead of the Authorized Agent Form.

Authentication/Verification. To help protect your privacy and maintain security when you submit a privacy request, we are required to reasonably validate your identity. To fulfill your request, we may require you to sign a declaration under penalty of perjury that you are the consumer whose Personal Data is the subject of the request. If we cannot validate the requestor based on the information provided, we will notify the requestor that we are unable to fulfill the request. We will only use Personal Data provided in the request to verify the requestor's identity or authority to make it. We will confirm receipt of a request within ten (10) business days. We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period. We do not charge a fee to process or respond to a verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will detail why we made that decision and provide a cost estimate before completing the request.

Declining Requests. Except for the automated controls described in this Notice, if you send us a request to exercise your rights or the choices in this section, to the extent permitted by applicable law, we may charge a fee or decline requests in certain cases. For example, we may decline requests where granting the request would be prohibited by law, could adversely affect the privacy or rights of another person, would reveal a trade secret or other confidential information, would interfere with a legal or business obligation that requires retention or use of the data, or because the data at issue is not covered under the law you are asserting.

Appeal. You have the right to appeal our decision to refuse to act on a CPRA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to privacy@ouro.com for our Privacy Team to review your data subject request. Within 45 days, we will provide you with a written explanation of the justification for declining to act on your request. If you disagree with our explanation, you have the right to file a complaint with the State's Attorney General HERE.

Data Retention. We retain personal data for as long as necessary to provide the Services and fulfill the transactions you have requested, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for

different data types in the context of different Services, actual retention periods can vary significantly based on criteria such as user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

Notice of Financial Incentives. We may offer rewards or prizes for participation in certain activities that may be considered a "financial incentive". These activities may involve the collection of Personal Data. The categories of Personal Data we collect are limited to what information you provide us, but may include: identifiers, protected class/demographic information, commercial information, online activities, geolocation information (general and precise), sensory information, employment information, and inferences. Activities we engage in that may be considered as a financial incentive include surveys where we may provide compensation such as a gift card in exchange for your time and responses, or a prize through your participation in promotions and sweepstakes. Participation in these programs may be subject to separate terms and conditions. Your participation in these programs is voluntary and you can terminate at any time as explained in any applicable terms. When we offer gift cards in exchange for your participation in a survey or when we engage in promotions or sweepstakes, the amount provided is reasonably related to the value of the data you provide, which takes into account a number of factors, including, the anticipated benefit we receive such as product improvement, better understanding how you use our products, to enhance our understanding of consumer and market trends, increased consumer engagement, and the anticipated expenses we incur in relation to the collection, storage, and use of the information we receive. The value may vary across surveys, promotions, and sweepstakes.

Where we offer you a financial incentive for providing your Personal Data, our accompanying disclosure will provide:

1. A succinct summary of the financial incentive or price or service difference offered;

2. A description of the material terms of the financial incentive or price or service difference, including the categories of Personal Data that are implicated by the financial incentive or price or service difference and the value of your Personal Data;

3. How the consumer can opt-in to the financial incentive or price or service difference;

4. A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

5. An explanation of how the financial incentive or price or service difference is reasonably related to the value of your Personal Data.

Contact Information. If you have any comments, concerns, or questions about this Privacy Policy, please contact us at privacy@ouro.com.