

Ouro U.S. Privacy Notice

Updated: January 17, 2025, Effective: January 17, 2025

This Privacy 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, 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 Notice (“Notice”) describes the types of personal information 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.

California consumers can find specific disclosures, including “[Notice at Collection](#)” details, by clicking here. If you’re a California resident and apply for a job with us, please see our Ouro HR Privacy Notice.

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 “Insurance Provider”) 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. For your convenience, we have provided 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.](#)

Insurance Provider Privacy Notice

- [Privacy Notice for the Chubb Group of Insurance Companies](#)

Our U.S. Consumer Privacy Notice

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 Insurance Provider'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 Insurance Provider'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 Insurance Provider privacy notice is distributed annually to each customer, as required by applicable law, and available online as well.

Please note, State laws may provide additional privacy rights in addition to the generally applicable privacy rights described in this Notice. Please scroll to the bottom of the page or [click here](#) for more information on your State-specific rights.

Information We Collect

When you visit a Site, we collect information that identifies, describes, or is reasonably capable of being associated with you ("Personal Information" or "Personal Identifiable Information") and other information that does not identify you personally or contain personal identifiers ("Anonymous Information"). We define Personal Information 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 Information when it can be linked with other information to personally identify you. Personal Information 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 Information 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 Information we collect varies based on your relationship with us.

Personal Information We Collect Directly From You

In order to access our Services, we may collect Personal Information directly from you that includes:

- Identifiers and Contact Information. We may collect personal identifiers and contact information such as your name, social security number, address, email address, phone number;
- Government-Issued Identifiers. We also may collect information such as your driver's license number, social security number, or other government-issued identifiers;
- Account Details. If you register an account with us, we collect information such as your email, phone number, or user ID, and password used to login to your account;
- Policy or Claims Information. This includes policy information, claim information, including materials you submit as part of your claim, or other information you choose to provide us;
- Financial Information. We may collect information necessary to process transactions such as account transaction history, payment card information, direct deposit information, and information 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, including occupation, information about your employer, employee email address, and income details (such as source of income, approximate or expected income and how frequently you are paid);
- Commercial Information. We may also collect information about the products, services, or coverage you purchase, including interest in a product or service, purchasing or consuming tendencies, and receipts or records of purchase or enrollment in products or Services;
- Message Contents. We may collect your messages, email contents, or any other information you so choose to provide when interacting with our customer service or agents;
- Audio or Similar Information. If you speak with our customer service team by phone, we may collect a recording for quality assurance and training purposes;
- Preferences. We may also collect information about the types of Services you use, your communications preferences, wish lists and other preferences you may select in your account or profile; and
- Other Information. We also collect information when you voluntarily provide to us, including your photograph, if you choose to upload a picture to the Services; survey responses; participation in contests, or other prospective marketing forms or devices; suggestions for improvements; referrals; or any other actions you perform on the Services.

Other Personal Information We Collect:

In the performance of our Services, we may collect other Personal Information from other sources, including:

- Information provided by identity verification and fraud prevention platforms;
- Information provided by 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; and
- 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.

Information collected in connection with your application or use of a particular Financial Product is described in the applicable Bank's and Insurance Provider's privacy notice.

How We Collect Information

We may collect Personal Information from you directly:

- in connection with a potential application for a Financial Product submitted through a Site.
- when you complete and submit online forms or fields available at a Site.
- when you complete a survey.
- when you opt into the sharing of information through a prompt on our Site.

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

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

- 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 Identifiable Information.
- From de-identified or aggregated Personal Identifiable Information, including payment data associated with a Financial Product.

How We Use Your Information

As noted above, Personal Information provided through an application for or use of or interaction with a Financial Product is used solely to establish your customer relationship and is subject to the privacy notice governing the particular Financial Product you selected.

Personal Identifiable Information provided or collected through other venues on the Site may be used in the following ways:

- To respond to your inquiries or requests; and
- To send you Ouro marketing communications that we believe may interest you.

Ouro does not sell Personal Identifiable 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 may aggregate or de-identify your Personal Identifiable Information for these same purposes.

How We Share the Information We Obtain

We may share the information we obtain about you with our affiliates and subsidiaries; our Banks, our Insurance Providers; 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 information (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 information to the resulting entities); or (8) otherwise with your consent.

Security

We maintain organizational, technical, and physical safeguards designed to protect the Personal Identifiable Information 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 Information 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 information.

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

Various States have enacted privacy laws ("State Privacy Laws") that grant their residents rights to receive certain disclosures regarding the collection, use, and sharing of Personal Identifiable Information, as well as rights to control this information.

It is important to note that, unless otherwise noted below, State Privacy Laws exclude Personal Identifiable Information 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 Identifiable Information related to a financial account.

Right of Access, Opt-out, and Deletion

Subject to exceptions under Federal law, where granted by State law, you have the right to request a copy or deletion of (i) the Categories of Personal Information that we've collect about you, (ii) the Specific Pieces of Personal Information we've collected about you, (iii) the

Categories of Sources from which we collect your Personal Information, (iv) the purpose for collecting your Personal Information, and (v) the Categories of Third Parties to whom we disclosed your Personal Information.

Making an Access or Deletion Request

You may make an access or deletion request, you can call 1-866-387-7363, write Ouro Customer Service, P.O. Box 2136, Austin, TX 78768-2136, or email customerservice@netspend.com.

At any time and without prior notice, we reserve the right to not accept requests from individuals that are outside the legal protections of their resident State.

For your security purposes, we verify your identity before we are able to process your access or deletion request. As such, we may ask you to provide such additional information as your first and last name, address, telephone number, email address, or other personal identifiers. This information will only be used for verification purposes.

Once we have verified your identity we will respond to your request as appropriate. For access requests, the requested information will be sent to you. For deletion requests, we may seek to confirm whether your request is for us to delete your Personal Identifiable Information or opt you out of receiving marketing. Opting you out of receiving marketing allows us to maintain your Personal Information but flag it so that you do not receive further offers from Ouro. If we do not maintain this flag, we will no longer have any record of you after fulfilling your opt-out request, and it is possible that we may again receive your information from one of our lead generation partners, in which case you could receive marketing from us again. We explain this in order to ensure we are meeting consumers' preferences. If we are unable to confirm your request, we will default to deleting your Personal Identifiable Information.

Please allow up to 45 days for a response to access and deletion requests.

Submitting a Sale, Share, or Targeted Advertising Opt-Out Request

If you live in a state that offers sale, share, or targeted advertising opt-outs, you can make that by submitting a request to customerservice@netspend.com.

Note to customers and consumers of Ouro's Bank partners:

You have secure direct online access to your own Personal Information, including profile and commercial or transactional history, via account tools and settings associated with your account. To determine which Bank is associated with your account, please see the back of your card or your account mobile app.

Non-discrimination

We do not provide a different level or quality of experience, or deny goods or services to you when you exercise your State rights.

Notice to California Residents

If you are a California resident, you have rights regarding your “Personal Information”. Under the California Consumer Privacy Act (“CCPA”), as amended and expanded by the California Privacy Rights Act (“CPRA”), TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100], “Personal Information” means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, 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,. “Personal Information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Your rights under California law are described below:

1. Notice of Collection

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 Information 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 information 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 Information**
 - **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.
 - **Sensitive demographic data.** Racial or ethnic origin, religious or philosophical beliefs, or union membership.
 - **Biometric information.** We do not collect biometric information.

2. Sources of Personal Information

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

- Directly from you, such as when you sign up for an account or contact member services, or participate in, sweepstakes, promotions, or research or survey activities;
- Our Bank and Insurance Providers;
- Your devices, when you use our Site or App;
- Your family or friends, such as when they provide us with your contact information by choosing to share their phone contacts with Ouro;
- Payment processors;
- External banks (i.e., banks other than our Banks) if you link a non Ouro-serviced account;
- Our affiliates and subsidiaries;
- Vendors who provide services on our behalf;

- Our joint marketing partners;
- Our business partners (such as referring websites);
- Online advertising services and advertising networks;
- Data analytics providers;
- Government entities;
- Operating systems and platforms;
- Social networks;
- Data brokers;
- Data aggregators.

In order for Ouro 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. Ouro keeps a record of your opt-in to ensure that we are not marketing to prospects without consent.

If you have received direct marketing from Ouro, there are cases where Ouro is not able to determine a prospect's current contact information with the information provided by our lead generation partners. In those cases, Ouro uses 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, Ouro has 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.

Ouro does not Sell Personal Information as that term is defined in the CCPA/CPRA.

3. Notice of Use of Personal Information

We may use (and may have used during the 12-month period prior to the effective date of this Statement) your Personal Information for the purposes described in the "How We Use Your Information" section above and for the following business purposes specified in the CCPA/CPRA:

- Performing Services, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing advertising or marketing services, providing analytics services, or providing similar services;
- Auditing related to a current interaction with you and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance;
- Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of your interaction with us, provided that your Personal Information is not disclosed to another third party and is not used to build a profile about you or otherwise alter your experience outside our interaction.

- Helping to ensure security and integrity by detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;
- Debugging to identify and repair errors that impair existing intended functionality;
- Undertaking internal research for technological development and demonstration;
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

4. Categories of third parties with whom Personal Information was shared

Subject to your consent, during the 12-month period prior to the effective date of this Statement, we may have shared your Personal Information with certain categories of third parties, as described below. When we share Personal Information with our Banks or Insurance Providers, we do so as their service provider. The privacy practices of our Bank Partners and Insurance Providers are subject to their privacy notices, which we strongly suggest you review. Ouro is not responsible for the information practices or privacy notices of our Banks and Insurance Providers. We may have disclosed the following categories of Personal Information about you for a business purpose to the following categories of third parties:

Category of Personal Information	Category of Third Party
Identifiers	Our Banks, our Insurance Providers, our marketing partners, and for paycards your employer
Additional Data Subject to Cal. Civ. Code § 1798.80 Law	Our Banks, our Insurance Providers, our marketing partners
Protected Classifications	Our Banks, our Insurance Providers, our marketing partners
Commercial Information	Our Banks Issuers, our Insurance Providers, our marketing partners
Biometric Information	We do not collect

Category of Personal Information	Category of Third Party
Online Activity	Our Banks, our Insurance Providers, our marketing partners
Geolocation data	Our Banks, our Insurance Providers
Sensory Information	Our Banks, our Insurance Providers
Employment Information	Our Banks, our Insurance Providers

In addition to the categories of third parties identified above, during the 12-month period prior to the effective date of this Statement, we may have shared Personal Information about you with the following additional categories of third parties: government entities; other persons to whom we have a legal obligation to disclose Personal Information (including, for example, in response to a duly issued subpoena or search warrant); and other persons to whom you authorize Ouro to disclose your Personal Information.

5. California Privacy Rights

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

- Access. You have a right to request that we disclose to you, twice in a 12-month period, the Personal Information we have collected about you. You also have a right to request additional information about our collection, use, disclosure, or sale of such Personal information, which is also provided in this privacy statement.
- Correction. You have the right to request that we correct inaccurate personal information under certain circumstances, subject to a number of exceptions.
- Deletion. You have the right to request that we delete your personal information under certain circumstances, subject to a number of exceptions.
- Opt-Out of the Selling or Sharing of your Data. You have the right to opt out of the selling or sharing of your data. To opt-out, submit your privacy request to Ouro at P.O. Box 2136, Austin, TX 78768-2136, email: customerservice@netspend.com, Tel: 1-866-387-7363. We may request certain information to verify your identity to complete your request. The CCPA/CPRA requires us to describe the categories of personal information we sell or share to third parties and how to opt-out of future sales. It is important to know that the 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. Ouro does not provide information that you might typically think of as personal information to

third parties in exchange for money; however, under the CCPA/CPRA, personal information 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 information available to third parties in some cases. “Share” is defined as providing personal information to a third party to target advertising to a consumer based on information about their activity on multiple websites across the internet. In the last 12 months, when you access our online 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 online Services and advertisements. We do not knowingly sell or share the personal information of minors under 18 years of age.

- Shine the Light Request. You have the right to request that we provide you with (a) a list of certain categories of personal information we have disclosed to third parties for their direct marketing purposes during the immediately preceding calendar year and (b) the identity of those third parties.
- Joint Marketing with other Financial Institutions. You have the right to opt-out of joint marketing with other financial institutions as well as limit the use of your Sensitive Personal Information. If you would like to opt out of joint marketing with other financial institutions by submitting a request to Ouro at P.O. Box 2136, Austin, TX 78768-2136, email: customerservice@netspend.com, Tel: 1-866-387-7363.
- Appeal. You have the right to appeal our decision to refuse to act on a CCPA/CPRA data privacy request within a reasonable period after you receive our decision. To appeal our decision, forward your denial email to mailto: customerservice@netspend.com for Ouro’s 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.
- Non-Discrimination. You have the right to not be discriminated against for exercising any of your privacy rights.
- Authentication/Verification. To help protect your privacy and maintain security, we will take steps to verify your identity before granting you access to your personal information or complying with your request (except for a request to opt-out of sales or sharing). We may require you to provide any of the following information: your name, date of birth, the last four digits of your Social Security number, the email and physical addresses associated with your Ouro account, one or more recent transactions, and the last four digits of one or more Ouro-serviced cards associated with your account. If you ask us to provide you with specific pieces of personal information, we may require you to sign a declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request. Further, we may decline a request where we are unable to authenticate you as the person to whom the data relates, the request is unreasonable or excessive, or where otherwise permitted by applicable law.

- **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.** Ouro may offer rewards or prizes for participation in certain activities that may be considered a “financial incentive” under California law. These activities may involve the collection of personal information. The categories of personal information we collect is 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 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.
- **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.

Changes to this Notice

Ouro may change this Notice at any time by posting an updated version to this page and changing the “Effective Date” at the top of this Notice. Any changes become effective when

posted on the Site. You will be bound by changes if you use the Site after those changes have been posted.

Questions?

If you have questions about this U.S. Consumer Notice, please contact us at:

Ouro Customer Service

P.O. Box 2136

Austin, TX 78768-2136

Email: customerservice@netspend.com

Tel: 1-866-387-7363